PCT/JP03/04808

日本国特許庁
JAPAN PATENT OFFICE

16.04.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　４月２３日

出願番号
Application Number: 特願２００２－１２０４３０
[ST.10/C]: [ＪＰ２００２－１２０４３０]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　５月２７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０３８９５６

【書類名】　特許願

【整理番号】　2032740027

【提出日】　平成14年 4月23日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 9/06

G06F 15/16

G06F 12/14

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　前田　卓治

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　三浦　康史

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　徳田　克己

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井上　信治

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　プログラム更新及び管理方法

【特許請求の範囲】

【請求項１】情報処理端末を一意に識別する端末ＩＤを外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、前記情報処理端末で動作するプログラム、前記プログラムに関する情報を格納したプログラムヘッダ、前記プログラムが使用する固有の情報であるプログラム固有情報、前記プログラム固有情報に関する情報を格納した固有情報ヘッダを保持するサーバ装置との間で行われるプログラム更新及び管理方法であって、

前記情報処理端末は、前記サーバ装置に対して前記端末ＩＤを含んだプログラム配布要求を行い、

前記サーバ装置は、前記プログラム配布要求に対して前記プログラム、前記プログラムヘッダ、前記プログラム固有情報、前記固有情報ヘッダを配布することを特徴とするプログラム更新及び管理方法。

【請求項２】前記情報処理端末はさらに、

前記情報処理端末内の外部から書き換えが行えない不揮発性メモリに前記情報処理端末毎に異なる固有鍵を格納し、

前記サーバ装置から取得した前記プログラムを、前記固有鍵を用いて暗号化して前記情報処理端末内に格納することを特徴とする請求項１記載のプログラム更新及び管理方法。

【請求項３】前記プログラムヘッダは前記プログラムを一意に特定することが可能な認証子を含み、前記固有鍵で暗号化され前記情報処理端末内に格納されているプログラムを前記固有鍵で復号し、前記認証子を用いて固有鍵での暗号化が正しく行われたことを確認することを特徴とする請求項２記載のプログラム更新及び管理方法。

【請求項４】前記プログラム、前記プログラムヘッダ、前記プログラム固有情報、前記固有情報ヘッダは電子的な署名が付加されていることを特徴とする請求項１から請求項３のいずれか１項に記載のプログラム更新及び管理方法。

【請求項５】前記プログラムヘッダは前記プログラムを一意に特定することが

可能な認証子を含み、前記固有情報ヘッダは前記プログラム固有情報を一意に特定することが可能な認証子を含み、前記プログラムヘッダ、前記固有情報ヘッダは電子的な署名が付加されていることを特徴とする請求項１から請求項３のいずれか１項に記載のプログラム更新及び管理方法。

【請求項６】情報処理端末を一意に識別する端末ＩＤを外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、前記プログラム固有情報を配布した情報処理端末を一意に識別する端末ＩＤと前記情報処理端末に配布した前記プログラム固有情報を一意に識別するプログラム固有情報ＩＤの対応を示す固有情報配布履歴を保持するサーバ装置との間で行われるプログラム更新及び管理方法であって、

前記情報処理端末からの端末ＩＤを指定したプログラム配布要求に対し、前記固有情報配布履歴に記載されている情報処理端末からの要求であれば前記プログラムのみを配布し、

前記固有情報配布履歴に記載されていない情報処理端末からの要求であれば前記プログラムと共に新規に前記プログラム固有情報を割り当てて配布し、

前記固有情報配布履歴に前記端末ＩＤ、前記プログラム固有情報ＩＤの対応関係を追加することを特徴とするプログラム更新及び管理方法。

【請求項７】前記プログラム固有情報は特定のプログラムに関連付けられた情報であり、前記プログラム固有情報ＩＤと前記プログラムを一意に識別するプログラムＩＤの対応を示すプログラム／固有情報対応表と、前記固有情報配布履歴を保持するサーバ装置において、前記情報処理端末からの端末ＩＤとプログラムＩＤを指定したプログラム配布要求に対し、前記プログラム／固有情報対応表と前記固有情報配布履歴を参照し、指定された前記プログラムＩＤに対応する前記プログラム固有情報を前記情報処理端末に配布済みであれば前記プログラムのみを配布し、配布していなければプログラムと共に新規に前記プログラム固有情報を割り当てて配布し、前記固有情報配布履歴に前記端末ＩＤ、前記プログラム固有情報ＩＤの対応関係を追加することを特徴とする請求項６記載のプログラム更新及び管理方法。

【請求項８】情報処理端末を一意に識別する端末ＩＤを外部から書き換えが行

えない不揮発性メモリに格納する情報処理端末と、前記プログラム固有情報を配布した情報処理端末を一意に識別する端末ＩＤと、前記端末ＩＤを持つ情報処理端末に対してプログラム固有情報を配布した回数の対応を示す配布回数情報を保持するサーバ装置との間で行われるプログラム更新及び管理方法であって、

前記情報処理端末からの端末ＩＤを指定したプログラム配布要求に対し、前記配布回数情報に記載されている配布回数が規定値以上であれば前記プログラムのみを配布し、規定値未満であれば前記プログラムと共に新規に前記プログラム固有情報を割り当てて配布し、前記配布回数情報に記載されている配布回数を更新することを特徴とするプログラム更新及び管理方法。

【請求項９】前記プログラム固有情報は特定のプログラムに関連付けられた情報であり、前記プログラム固有情報ＩＤと前記プログラムを一意に識別するプログラムＩＤの対応を示すプログラム／固有情報対応表と、前記配布回数情報を保持するサーバ装置において、前記情報処理端末からの端末ＩＤとプログラムＩＤを指定したプログラム配布要求に対し、前記プログラム／固有情報対応表と前記配布回数情報を参照し、指定された前記プログラムＩＤに対応する前記プログラム固有情報を前記情報処理端末に配布した回数が規定値以上であれば前記プログラムのみを配布し、規定値未満であればプログラムと共に新規に前記プログラム固有情報を割り当てて配布し、前記配布回数情報に記載されている配布回数を更新することを特徴とする請求項８記載のプログラム更新及び管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理端末で動作するプログラムの更新方法に関し、プログラムの配布方法、ならびに配布したプログラムの管理方法に関する。

【０００２】

【従来の技術】

近年、携帯電話からのインターネット接続や、デジタルＴＶの放送開始など、ネットワークサービスに対応した組込み機器が登場し、注目を浴びている。ネットワーク技術の発展によりネットワークのブロードバンド化が進む中、ネットワ

ークサービスに対応した組込み機器は今後さらに登場するものと考えられる。

【０００３】

組込み機器のネットワーク化に伴い機器が急速に高機能化されるにつれ、各機器に搭載されるソフトウェアの規模は飛躍的に増大している。ソフトウェアの大規模化は、開発人員の増加、開発工数の長期化などの諸問題を引き起こす。また、ネットワークサービス提供者間の競争により新規サービスが次々と登場する中、端末メーカーも新規サービスに対応した新機種を短期間で開発することが求められており、機器の開発サイクルは短くなってきている。

【０００４】

このような背景により、端末メーカーは大規模なソフトウェアを短期間に開発、テストし、商品を出荷する必要があり、結果として機器に対する十分なテストが行えないまま市場に出荷され、後日ソフトウェアの不具合が発覚し、商品回収を行うというケースも増加している。

【０００５】

従来、組込み機器におけるプログラムの不具合修正方法としては、商品を回収してプログラムを入れ替える方法が存在する。商品を回収してプログラムを入れ替える方法では、回収した商品に対しプログラムを格納しているＲＯＭを張り替えたり、プログラムを格納しているＦｌａｓｈメモリのプログラムを新しいプログラムに書き換えたりすることで、プログラムの不具合修正を行う。この方法では、ユーザが店頭に商品を持参する、商品をメーカーに送付するなどの必要がありユーザにかかる負担は大きい。また、回収コストも膨大になるため、ユーザ、メーカーの両者にとって商品を回収せずに修正する方法が望ましい。

【０００６】

一方、組込み機器がネットワークに接続されることにより、ネットワークから様々なデータを取得し、ネットワークを用いたサービスを利用することが可能になる。例えばホームページの閲覧や、電子メールの送受信、音楽・画像などのコンテンツ配信サービスなど、従来ＰＣで実現されていたネットワークサービスが組込み機器で実現できるほか、組込み機器の機能と組み合わせた新規サービスの実現も可能となる。また、ネットワークから取得する情報はデータだけではなく

、プログラムを取得することも可能である。そのため、従来機器の回収という形で行ってきたプログラムの不具合修正を、ネットワーク経由のプログラム配信により実現することが可能になる。また、従来ＰＣで行われてきた、ネットワーク経由のプログラム追加による機能追加を組込み機器で実現することも可能になる。

【０００７】

【発明が解決しようとする課題】

電子ショッピングやコンテンツ配信サービスなど、課金を伴う商用システムを実現する場合、悪意のあるユーザが不正にプログラムを書き換えることが可能であれば、課金情報の操作により無料で商品やコンテンツを購入するなどの不正行為が行われる可能性がある。そのため、ネットワーク経由のプログラム更新による不具合修正、追加を行う場合、悪意のあるユーザが不正に改ざんしたプログラムを機器に取り込まないよう、プログラムの正当性を検証する必要がある。

【０００８】

従来プログラムの正当性を検証する方法として、特開２０００－３３９１５３号公報に示されるような電子的な署名を用いる方法が存在する。この方法では、公開鍵暗号方式と呼ばれる２つの対となる鍵の組を用いた暗号化データ交換方式を利用する。署名を用いたプログラムの正当性検証方法に関して、図１を用いて説明する。同図において、１００はプログラムを開発し配布するプログラム発行者、１１０はプログラム発行元の身元を確認し保証する第三者認証機関であるＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）、１２０はプログラムを取得するユーザを示す。プログラム発行者１００は、公開鍵１０１、秘密鍵１０２と呼ばれる２つの鍵を保有する。秘密鍵１０２はプログラム発行者１００のみが知り得る鍵であり、プログラム発行者１００が秘匿情報として管理する。公開鍵１０１は他者に公開するための鍵であり、公開しても秘密鍵１０２の内容は予測できない仕組みとなっている。ＣＡ１１０はプログラム発行者１００と同じく、ＣＡ公開鍵１１１、ＣＡ秘密鍵１１２の２つの鍵を保有する。

【０００９】

プログラム正当性検証の手順は次の通り。

【００１０】

（１）プログラム発行者１００はＣＡ１１０に公開鍵１０１を送付する。

【００１１】

（２）ＣＡ１１０は、プログラム発行者１００の身元を確認、審査する。

【００１２】

（３）ＣＡ１１０がプログラム発行者１００を信頼できると判断した場合、プログラム発行者１００の公開鍵１０１に対しＣＡ秘密鍵１１２で電子的な署名を行った証明書を発行する。証明書は公開鍵保有者の身元を識別する情報を含み、第三者認証機関であるＣＡ１１０が公開鍵保有者の身元を保証するものである。

【００１３】

（４）ＣＡ１１０は、プログラム発行者１００にプログラム発行者の公開鍵証明書１０３を送付する。

【００１４】

（５）プログラム発行者１００は配布するプログラムに対し、自己の秘密鍵１０１で電子的な署名を行う。

【００１５】

（６）プログラム発行者１００はユーザ１２０に対し、公開鍵証明書１０３、署名付きプログラム１０４を配布する。

【００１６】

（７）ユーザ１２０はＣＡ１１０からＣＡ公開鍵１１１を取得する。

【００１７】

（８）ユーザ１２０は、ＣＡ公開鍵１１１を用いてプログラム発行者の公開鍵証明書１０３の署名を検証する。

【００１８】

（９）署名の検証が正しく行われた場合、公開鍵証明書１０３に含まれる公開鍵１０１を用いて署名付きプログラム１０４の署名を検証する。

【００１９】

（１０）署名の検証が正しく行われた場合、配布されたプログラムがプログラム発行者１００から配布されたプログラムであり、改ざんされていないことを検

証できる。上記の公開鍵暗号方式及び証明書、署名、認証の仕組みに関しては、「Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」Ｂｒｕｃｅ　Ｓｃｈｎｅｉｅｒ，Ｊｏｈｎ　Ｗｉｌｅｙ　＆　Ｓｏｎｓ，Ｉｎｃ（１９９６）が詳しい。

【００２０】

ここで説明した方法では、文書に手書きの署名を付加し、正当性を保証するのと同様に、プログラムに電子的な署名を付加することによりプログラムの正当性を保証している。これにより、ユーザ１２０はプログラムが配布元から発行された正当なものであることを検証できる。

【００２１】

しかしながら、図１に示した例では配布時におけるプログラムの正当性検証は行えるが、配布後のプログラムに関して正当性を保証することはできない。この問題点を解決する方法として、特開平７－２９５８００号公報が存在する。特開平７－２９５８００号公報に示された方法は、プログラム配布先のユーザ識別子を用いてプログラム配布元でプログラムを暗号化して配布し、ユーザは使用時にユーザ識別子を用いてプログラムを復号化して実行する方法である。この方法では、万が一プログラムが不正にコピーされたとしても、ユーザ識別子が一致しなければプログラムを復号し実行することができないため、不正コピー、不正改ざんを防止することが可能となる。しかしながら、プログラム配布元で各ユーザ識別子に応じた暗号処理を行う必要があり、プログラム配布元にかかる負担は大きい。

【００２２】

一方、ネットワークを用いた電子ショッピングや、コンテンツ配信サービスなど、課金を伴う商用システムを実現する場合、ユーザを特定する方法が必要となる。そのため、プログラムあるいはプログラムと共に配布する情報の中に、ユーザ毎に割り当てるＩＤや鍵などの固有情報を含ませる場合がある。この場合、ユーザに固有情報を割り当て、管理することで、ユーザが不正行為を行った際に固有情報を元にユーザを特定することが可能となる。不正ユーザを特定すれば、不正ユーザが使用する固有情報を無効にすることで、不正行為を防止することが可能となる。

【００２３】

この固有情報を用いた不正行為を防止する方法では、１ユーザが複数の固有情報を取得することが可能であれば、不正ユーザとして排除されたユーザが再度別の固有情報を取得することで、新たなユーザとして識別され、更に不正行為を繰り返すことが可能となるため。そのため、不正ユーザが複数の固有情報を取得できないようにする仕組みが必要となる。

【００２４】

本発明では上記問題点に鑑み、プログラム配布元の負担が少ないプログラムの不正コピーや不正改ざんを防ぐ方法を提供すると共に、固有情報のユーザへの配布回数を制限することで不正行為を防止することが可能なプログラム更新及び管理方法を提供することを目的とする。

【００２５】

【課題を解決するための手段】

前記課題を解決するために第１の発明は、情報処理端末を一意に識別する端末ＩＤと、情報処理端末毎に異なる固有鍵を外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、情報処理端末で動作するプログラム、プログラムに関する情報を格納したプログラムヘッダ、プログラムが使用する固有の情報であるプログラム固有情報、プログラム固有情報に関する情報を格納した固有情報ヘッダを保持するサーバ装置において、情報処理端末の端末ＩＤを含んだプログラム配布要求に対し、それぞれ電子的な署名が付加されたプログラム、プログラムヘッダ、プログラム固有情報、固有情報ヘッダを配布し、情報処理端末内でプログラムを固有鍵で暗号化し格納することを特徴とする。

【００２６】

前記課題を解決するために第２の発明は、プログラムヘッダにプログラムを一意に特定することが可能な認証子を含み、固有情報ヘッダにプログラム固有情報を一意に特定することが可能な認証子を含み、プログラムヘッダと固有情報ヘッダに電子的な署名を付加することを特徴とする。

【００２７】

前記課題を解決するために第３の発明は、プログラム固有情報を配布した情報

処理端末を一意に識別する端末ＩＤと、情報処理端末に配布したプログラム固有情報を一意に識別するプログラム固有情報ＩＤの対応を管理する固有情報配布履歴を保持するサーバ装置において、情報処理端末からの端末ＩＤを指定したプログラム配布要求に対し、固有情報配布履歴に記載されている情報処理端末からの要求であればプログラムのみを配布し、固有情報配布履歴に記載されていない情報処理端末からの要求であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、固有情報配布履歴に端末ＩＤ、プログラム固有情報ＩＤの対応関係を追加することを特徴とする。

【００２８】

前記課題を解決するために第４の発明は、プログラム固有情報を一意に識別するプログラム固有情報ＩＤと、プログラムを一意に識別するプログラムＩＤの対応を示すプログラム／固有情報対応表と、固有情報配布履歴を保持するサーバ装置において、情報処理端末からの端末ＩＤとプログラムＩＤを指定したプログラム配布要求に対し、プログラム／固有情報対応表と固有情報配布履歴を参照し、指定されたプログラムＩＤに対応するプログラム固有情報を配布済みの情報処理端末からの要求であればプログラムのみを配布し、配布していない情報処理端末からの要求であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、固有情報配布履歴に端末ＩＤ、プログラム固有情報ＩＤの対応関係を追加することを特徴とする。

【００２９】

前記課題を解決するために第５の発明は、プログラムが使用するプログラム固有情報を配布した情報処理端末を一意に識別する端末ＩＤと、プログラム固有情報を配布した回数を示す配布回数情報を保持するサーバ装置において、情報処理端末からの端末ＩＤを指定したプログラム配布要求に対し、配布回数情報に記載されている配布回数が規定値以上であればプログラムのみを配布し、規定値未満であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、配布回数情報に記載されている配布回数を更新することを特徴とする。

【００３０】

前記課題を解決するために第６の発明は、プログラム固有情報を一意に識別す

るプログラム固有情報ＩＤと、プログラムを一意に識別するプログラムＩＤの対応を示すプログラム／固有情報対応表と、配布回数情報を保持するサーバ装置において、情報処理端末からの端末ＩＤとプログラムＩＤを指定したプログラム配布要求に対し、プログラム／固有情報対応表と配布回数情報を参照し、指定されたプログラムＩＤに対応するプログラム固有情報を情報処理端末に配布した回数が規定値以上であればプログラムのみを配布し、規定値未満であればプログラムと共に新規にプログラム固有情報を割り当てて配布し、配布回数情報に記載されている配布回数を更新することを特徴とする。

【００３１】

【発明の実施の形態】

以下、本発明のプログラム更新及び管理方法について、図を用いて説明する。

【００３２】

（実施の形態１）

図２は本発明の実施の形態１における情報処理端末とサーバ装置の構成図であり、同図において、２００は情報処理端末、２２０はサーバ装置を示している。情報処理端末２００は、ＣＰＵ２０１、ＲＡＭ２０２、プログラムやデータなどの暗号化及び復号化処理を行う暗号処理部２０３、サーバ装置２２０との通信を行う通信処理部２０４、プログラムを格納するプログラム格納部２０５、ＣＡ公開鍵など特に秘匿する必要がない情報を格納するデータ格納部２０６、秘密鍵など秘匿する必要がある情報を格納する秘匿情報格納部２０７から構成されている。プログラム格納部２０５には、ＣＰＵ２０１で動作するプログラム２１６が格納されている。データ格納部２０６は、情報処理端末２００で使用されるデータのうち特に秘匿する必要がないものが格納されており、情報処理端末２００に格納されているプログラムのＩＤやバージョン番号など格納プログラムの管理情報であるプログラム管理情報２０８、ＣＡ公開鍵２０９が格納されている。また、秘匿情報格納部２０７は、情報処理端末２００内で秘匿する必要がある情報が格納されており、情報処理端末毎に異なる鍵である端末固有鍵２１０、情報処理端末毎に異なる公開鍵ペアの１つである端末秘密鍵２１１、プログラムが使用する固有鍵などのプログラム固有情報２１２、情報処理端末毎に異なる公開鍵ペアの

他方である端末公開鍵証明書２１３が格納されている。端末公開鍵証明書２１３は情報処理端末を一意に識別するＩＤである端末ＩＤ２１４、端末公開鍵証明書に対しＣＡが付加したＣＡ署名２１５を含んでいる。

【００３３】

一方サーバ装置２２０は、ＣＰＵ２２１、ＲＡＭ２２２、プログラムやデータなどの暗号化及び復号化処理を行う暗号処理部２２３、情報処理端末２００との通信を行う通信処理部２２４、ＣＡ公開鍵など特に秘匿する必要がない情報を格納するデータ格納部２２５、情報処理端末２００に配布するプログラムなどの情報を格納する配布情報格納部２２６から構成されている。さらにデータ格納部２２５はサーバ装置２２０が使用する情報を格納する領域であり、公開鍵ペアの１つであるサーバ秘密鍵２２７、公開鍵ペアの他方であるサーバ公開鍵証明書２２８、ＣＡ公開鍵２２９が格納されている。サーバ公開鍵証明書２２８はサーバを一意に識別するＩＤであるサーバＩＤ２３０、サーバ公開鍵証明書に対しＣＡが付加したＣＡ署名２３１を含んでいる。配布情報格納部２２６は、サーバ装置２２０が情報処理端末２００に対して配布する情報を格納する領域であり、プログラムヘッダ２３２、プログラム２３３、固有情報ヘッダ２３４、プログラム固有情報２３５が格納されている。

【００３４】

配布情報格納部２２６に格納されているプログラムヘッダ２３２、プログラム２３３、固有情報ヘッダ２３４、プログラム固有情報２３５には第三者認証機関であるＣＡの署名が付加されており、配布情報が正当な配布元から配布されるものであることを保証している。

【００３５】

次に図３を用いて、プログラムヘッダとプログラムの関係を説明する。

【００３６】

プログラムヘッダ３００は、プログラム３１０に関する情報を格納するものである。プログラムヘッダ３００は、次の情報を含む。

【００３７】

（１）プログラムヘッダ３００が格納する情報がどのプログラム３１０に対応

した情報かを示すプログラムＩＤ（３０１）。

【００３８】

（２）対応するプログラム３１０のバージョン番号（３０２）。

【００３９】

（３）対応するプログラム３１０のプログラムサイズ（３０３）。

【００４０】

（４）対応するプログラム３１０のハッシュ値（３０４）。

【００４１】

（５）上記（１）から（４）までの情報を含むプログラムヘッダ３００全体に対するＣＡの署名（３０５）。

【００４２】

また、プログラム３１０は、プログラム３１０に対するＣＡの署名（３１１）が付加されている。

【００４３】

このようにプログラムヘッダ３００、プログラム３１０は共にＣＡの署名を含むため、情報処理端末２００においてプログラムヘッダ、プログラムが正当な配布元から配布されたものであることを検証することが可能である。

【００４４】

同様に図４を用いて、固有情報ヘッダとプログラム固有情報の関係を説明する。

【００４５】

固有情報ヘッダ４００は、プログラム固有情報４２０に関する情報を格納するものである。固有情報ヘッダ４００は、次の情報を含む。

【００４６】

（１）固有情報ヘッダ４００が格納する情報がどのプログラム固有情報４２０に対応した情報かを示すプログラム固有情報ＩＤ（４０１）。

【００４７】

（２）対応するプログラム固有情報４２０を使用するプログラムのプログラムＩＤ（４０２）。

【００４８】

（３）対応するプログラム固有情報４２０が格納する固有情報の数（４０３）。

【００４９】

（４）対応するプログラム固有情報４２０全体のサイズ（４０４）。

【００５０】

（５）対応するプログラム固有情報４２０に含まれる個々の固有情報に関する情報を示す固有情報サブヘッダ（４０５）。固有情報サブヘッダ４０５はプログラム固有情報４２０に含まれる個々の固有情報の数だけ存在する。

【００５１】

（６）上記（１）から（５）までの情報を含む固有情報ヘッダ４００全体に対するＣＡの署名（４０６）。

【００５２】

固有情報サブヘッダ４０５はさらに個々の固有情報を識別するためのＩＤであるプログラム固有情報サブＩＤ４１１、個々の固有情報のサイズ４１２から構成される。

【００５３】

また、プログラム固有情報４２０は、複数のプログラム固有情報（４２１）と、プログラム固有情報全体に対するＣＡの署名（４２２）を含む。

【００５４】

このように固有情報ヘッダ４００、プログラム固有情報４２０は共にＣＡの署名を含むため、情報処理端末２００において固有情報ヘッダ、プログラム固有情報が正当な配布元から配布されたものであることを検証することが可能である。

【００５５】

次に情報処理端末２００、サーバ装置２２０間で行われるプログラム更新手順の例を、図５を用いて説明する。

【００５６】

第１にＳ５０１において、情報処理端末２００とサーバ装置２２０はＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）による接続を行う。ＳＳＬは、２点

間でデータを安全に送受信するために、公開鍵暗号方式と秘密鍵暗号方式を併用して、データを暗号化して送受信する仕組みである。ＳＳＬの詳細はＮｅｔｓｃａｐｅ社から技術文書として公開されている。ＳＳＬではセッション鍵と呼ばれる鍵を共有するため、Ｓ５０２以降の情報処理端末２００とサーバ装置２２０間のデータ送受信は、すべてセッション鍵を用いた暗号化データにより行われる。

【００５７】

次にＳ５０２において、情報処理端末２００はサーバ装置２２０に対し、取得したいプログラム２３３のプログラムＩＤを指定してヘッダの取得を要求する。

【００５８】

Ｓ５０３において、ヘッダ取得要求を受信したサーバ装置２２０は、配布情報格納部２２６に格納したプログラムヘッダ２３２を情報処理端末２００に送信する。

【００５９】

Ｓ５０４において、サーバ装置２２０からプログラムヘッダ２３２を受信した情報処理端末２００は、データ格納部２０６に格納しているＣＡの公開鍵２０９を用いて、プログラムヘッダ２３２に含まれているＣＡの署名を検証する。これにより、情報処理端末２００はプログラムヘッダ２３２が改ざんされていない、正当な配布元から配布された情報であることを検証する。プログラムヘッダ２３２には、プログラムのプログラムＩＤ、バージョン番号、サイズ、プログラムのハッシュ値などプログラムに関する情報が格納されている。この情報と、データ格納部２０６に格納されているプログラム管理情報２０８内に記載されているプログラムＩＤ、バージョン情報、空き容量情報を比較し、更新対象のプログラムが正しくサーバ装置２２０から配布されたか、プログラムを格納する空き容量が存在するか確認する。

【００６０】

次にＳ５０５において、サーバ装置２２０は配布情報格納部２２６に格納した固有情報ヘッダ２３４を情報処理端末２００に送信する。

【００６１】

Ｓ５０６において、サーバ装置２２０から固有情報ヘッダ２３４を受信した情

報処理端末２００は、データ格納部２０６に格納しているＣＡの公開鍵２０９を用いて、固有情報ヘッダ２３４に含まれているＣＡの署名を検証する。これにより、情報処理端末２００は固有情報ヘッダ２３４が改ざんされていない、正当な配布元から配布された情報であることを検証する。固有情報ヘッダ２３４には、プログラム固有情報を一意に識別するプログラム固有情報ＩＤ、プログラム固有情報に関連するプログラムのプログラムＩＤ、プログラム固有情報で配布される情報に含まれる固有情報の数、サイズなどプログラム固有情報に関する情報が格納されている。この情報と、データ格納部２０６に格納されているプログラム管理情報２０８内に記載されているプログラムＩＤ、空き容量情報を比較し、更新対象のプログラムに関するプログラム固有情報が正しくサーバ装置２２０から配布されたか、プログラム固有情報を格納する空き容量が存在するか確認する。

【００６２】

Ｓ５０４、Ｓ５０６で情報処理端末２００が空き容量の確認を行い、プログラム、プログラム固有情報の取得が行えると判断した場合、Ｓ５０７において情報処理端末２００はサーバ装置２２０に対しプログラムＩＤを指定してプログラム取得を要求する。

【００６３】

Ｓ５０８において、プログラム取得要求を受信したサーバ装置２２０は、配布情報格納部２２６に格納したプログラム２３３を情報処理端末２００に送信する。

【００６４】

次にＳ５０９において、サーバ装置２２０からプログラム２３３を受信した情報処理端末２００は、データ格納部２０６に格納しているＣＡの公開鍵２０９を用いて、プログラム２３３に含まれているＣＡの署名を検証する。これにより、情報処理端末２００はプログラム２３３が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム２３３を秘匿情報格納部２０７に格納している端末固有鍵２１０で暗号化し、プログラム格納部２０５に格納する。その際、プログラム格納位置やプログラムＩＤ、バージョン番号などをプログラム管理情報２０８に格

納し、プログラムの管理を行う。

【００６５】

Ｓ５１０において、プログラムの格納が完了した後、プログラム格納部２０５に格納したプログラム２１６を、端末固有鍵２１０を用いて復号し、ハッシュ値を算出する。算出した値とプログラムヘッダ２３２に格納されているハッシュ値の比較を行い、プログラムが正しく格納されていることを確認する。

【００６６】

次にＳ５１１において情報処理端末２００はサーバ装置２２０に対しプログラムＩＤを指定してプログラム固有情報取得を要求する。

【００６７】

Ｓ５１２において、サーバ装置２２０は配布情報格納部２２６に格納したプログラム固有情報２３５を情報処理端末２００に送信する。

【００６８】

次にＳ５１３において、サーバ装置２２０からプログラム固有情報２３５を受信した情報処理端末２００は、データ格納部２０６に格納しているＣＡの公開鍵２０９を用いて、プログラム固有情報２３５に含まれているＣＡの署名を検証する。これにより、情報処理端末２００はプログラム固有情報が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム固有情報を秘匿情報格納部２０７に格納する。

【００６９】

プログラム、プログラム固有情報の格納が完了した後、通信を切断する（Ｓ５１４）。

【００７０】

図５で示した本発明のプログラム更新手順について、本発明の主眼となる点について説明する。

【００７１】

第１に情報処理端末２００においてプログラムを暗号化している点である。従来の方法ではサーバ装置２２０においてプログラムを情報処理端末２００固有の

鍵で暗号化していたため、サーバ装置２２０においてプログラムを暗号化する処理が必要であった。これに対し本発明では情報処理端末２００においてプログラムを暗号化しているため、サーバ装置２２０におけるプログラム暗号化処理の負担を軽減することが可能となる。

【００７２】

また、情報処理端末２００において情報処理端末２００固有の鍵である端末固有鍵２１０で暗号化した場合、正しく端末固有鍵２１０で暗号化が行えたことを確認する必要がある。この点に関し本発明では、プログラム格納後に端末固有鍵２１０で復号し、平文プログラムのハッシュ値による検証を行う。復号後のプログラムに対するハッシュ値を検証することで、情報処理端末２００毎に異なる端末固有鍵暗号化を意識することなく、プログラム格納の成否を判定することが可能となる。

【００７３】

第２にプログラムとプログラム固有情報を個別に作成している点である。端末毎に異なる情報であるプログラム固有情報は、複数端末に配布するため複数の情報を管理する必要があるが、プログラムを利用する全端末で共通な情報となるプログラムは１式のみ管理することになる。これにより、サーバ装置２２０で管理する配布情報の大きさを低減することが可能となり、サーバ装置２２０における情報管理の負担を軽減することが可能となる。

【００７４】

なお、本実施の形態では情報処理端末２００とサーバ装置２２０間でＳＳＬを用いた暗号化データの送受信を行っているが、２点間で安全にデータの送受信が行える方法であれば、ＳＳＬに限らず他のプロトコルを用いてもよい。また、本実施の形態ではデータ格納部２０６とプログラム格納部２０５を別にしているが、同一の格納部としてもよい。また、本実施の形態では秘匿情報格納部２０７に端末公開鍵証明書２１３を格納しているが、データ格納部２０６に格納してもよい。また、本実施の形態ではプログラムヘッダ、固有情報ヘッダをプログラム、プログラム固有情報とは別に作成しているが、プログラムとプログラムヘッダ、プログラム固有情報と固有情報ヘッダをそれぞれ一体の情報とし、サーバ装置２

２０からの配布に先立ちヘッダ部分のみ切り出して情報処理端末２００に送信してもよい。また、本実施の形態ではプログラム、プログラム固有情報に対し配布時にセッション鍵による暗号化を行う例を示したが、セッション鍵とは異なる鍵でさらに暗号化し、その鍵をプログラムヘッダ、固有情報ヘッダに含めて配布する構成としてもよい。また、本実施の形態でハッシュ値と記載している点は、ハッシュアルゴリズムとしてＳＨＡ－１、ＭＤ５などの既存のハッシュアルゴリズムを使用してもよいし、独自のアルゴリズムを用いてもよい。また、ハッシュアルゴリズムのかわりにチェックサムなどの方法を用いて改ざんの検出を行ってもよい。また、情報処理端末２００毎に異なる情報を必要としないプログラムを配布する場合は、プログラム固有情報の配布を行う必要はない。

【００７５】

（実施の形態２）

図６、図７は本発明の実施の形態２におけるサーバ装置２２０内の配布情報格納部２２６に格納されるデータを示す。情報処理端末２００とサーバ装置２２０の構成は、本発明の実施の形態１と同様、図２に示すものとする。

【００７６】

図６を用いて、プログラムヘッダとプログラムの関係を説明する。

【００７７】

プログラムヘッダ６００は、プログラム６１０に関する情報を格納するものである。プログラムヘッダ６００は、次の情報を含む。

【００７８】

（１）プログラムヘッダが格納する情報がどのプログラムに対応した情報かを示すプログラムＩＤ（６０１）。

【００７９】

（２）対応するプログラムのバージョン番号（６０２）。

【００８０】

（３）対応するプログラムのプログラムサイズ（６０３）。

【００８１】

（４）対応するプログラムのハッシュ値（６０４）。

【００８２】

（５）上記（１）から（４）までの情報を含むプログラムヘッダ全体に対するＣＡの署名（６０５）。

【００８３】

本発明の実施の形態１と異なる点は、プログラム６１０にＣＡの署名を付加しない点である。

【００８４】

プログラムヘッダ６００、プログラム６１０の正当性検証を情報処理端末２００において行う場合、次の手順で行う。

【００８５】

第１にプログラムヘッダ６００をサーバ装置２２０から取得し、プログラムヘッダ６００に付加されたＣＡの署名６０５を検証する。これにより、情報処理端末２００はプログラムヘッダ６００が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【００８６】

次にプログラム６１０のハッシュ値を算出する。算出したハッシュ値と、プログラムヘッダ６００に格納されているプログラムのハッシュ値６０４を比較し、一致することを確認する。これにより、情報処理端末２００はプログラム６１０が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【００８７】

このように、プログラム６１０の正当性検証にプログラムヘッダ６００に格納されたプログラムのハッシュ値６０４を使用し、プログラムヘッダ６００にのみＣＡ署名６０５を付加することで、ＣＡの署名を必要とする情報を低減しながら、プログラムヘッダ６００、プログラム６１０に署名を付加する場合と同様の効果を得ることが可能となる。

【００８８】

また、プログラムヘッダ６００とプログラム６１０の組み合わせが不正に変更された場合、情報処理端末２００において、プログラムのハッシュ値を算出する

ことにより組み合わせの異常を検出することが可能となる。

【００８９】

次に図７を用いて、固有情報ヘッダとプログラム固有情報の関係を説明する。

【００９０】

固有情報ヘッダ７００は、プログラム固有情報７２０に関する情報を格納するものである。固有情報ヘッダ７００は、次の情報を含む。

【００９１】

（１）固有情報ヘッダが格納する情報がどのプログラム固有情報に対応した情報かを示すプログラム固有情報ＩＤ（７０１）。

【００９２】

（２）対応するプログラム固有情報を使用するプログラムのプログラムＩＤ（７０２）。

【００９３】

（３）対応するプログラム固有情報が格納する固有情報の数（７０３）。

【００９４】

（４）対応するプログラム固有情報全体のサイズ（７０４）。

【００９５】

（５）対応するプログラム固有情報全体のハッシュ値（７０５）。

【００９６】

（６）対応するプログラム固有情報に含まれる個々の固有情報に関する情報を示す固有情報サブヘッダ（７０６）。固有情報サブヘッダ７０６はプログラム固有情報に含まれる個々の固有情報の数だけ存在する。

【００９７】

（７）上記（１）から（６）までの情報を含む固有情報ヘッダ全体に対するＣＡの署名（７０７）。

【００９８】

固有情報サブヘッダ７０６はさらに個々の固有情報を識別するためのＩＤであるプログラム固有情報サブＩＤ７１１、個々の固有情報のサイズ７１２から構成される。

【００９９】

本発明の実施の形態１と異なる点は、固有情報ヘッダ７００にプログラム固有情報７２０のハッシュ値を格納し、プログラム固有情報７２０にＣＡの署名を付加しない点である。

【０１００】

固有情報ヘッダ７００、プログラム固有情報７２０の正当性検証を情報処理端末２００において行う場合、次の手順で行う。

【０１０１】

第１に固有情報ヘッダ７００をサーバ装置２２０から取得し、固有情報ヘッダ７００に付加されたＣＡの署名７０７を検証する。これにより、情報処理端末２００は固有情報ヘッダ７００が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【０１０２】

次にプログラム固有情報７２０のハッシュ値を算出する。算出したハッシュ値と、固有情報ヘッダ７００に格納されているプログラム固有情報のハッシュ値７０５を比較し、一致することを確認する。これにより、情報処理端末２００はプログラム固有情報７２０が改ざんされていない、正当な配布元から配布された情報であることを検証する。

【０１０３】

このように、固有情報ヘッダ７００にプログラム固有情報のハッシュ値７０５を格納し、固有情報ヘッダ７００にのみＣＡ署名７０７を付加することで、ＣＡの署名を必要とする情報を低減しながら、固有情報ヘッダ７００、プログラム固有情報７２０に署名を付加する場合と同様の効果を得ることが可能となる。

【０１０４】

また、固有情報ヘッダ７００とプログラム固有情報７２０の組み合わせが不正に変更された場合、情報処理端末２００において、プログラム固有情報のハッシュ値を算出することにより組み合わせの異常を検出することが可能となる。

【０１０５】

なお、本実施の形態でハッシュ値と記載している点は、ハッシュアルゴリズム

としてＳＨＡ－１、ＭＤ５などの既存のハッシュアルゴリズムを使用してもよいし、独自のアルゴリズムを用いてもよい。また、ハッシュアルゴリズムのかわりにチェックサムなどの方法を用いて改ざんの検出を行ってもよい。

【０１０６】

（実施の形態３）

図８に本発明の実施の形態３における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態１と異なる点は、サーバ装置８２０がプログラム固有情報８３５を情報処理端末８００に配布した履歴を管理するための固有情報配布履歴８４０を保持する点である。

【０１０７】

固有情報配布履歴８４０の情報格納例を図９に示す。

【０１０８】

固有情報配布履歴９００は、プログラム固有情報８３５を配布した情報処理端末８００を識別するＩＤである端末ＩＤ９０１、配布したプログラム固有情報８３５を識別するＩＤであるプログラム固有情報ＩＤ９０２を格納する。また、必要に応じてプログラム固有情報８３５を最後に配布した日時を示す最終配布日付９０３を格納する。

【０１０９】

同図の例では、サーバ装置８２０は情報処理端末８００に５つのプログラム固有情報８３５を配布済みであり、それぞれの端末ＩＤ９０１、プログラム固有情報ＩＤ９０２の組は、（端末ＩＤ、プログラム固有情報ＩＤ）＝（０００１、０００１）、（０００２、０００２）、（００１０、０００３）、（００１５、０００４）、（００２０、０００５）となる。

【０１１０】

サーバ装置８２０における固有情報配布履歴８４０を用いたプログラム配布手順について図１０を用いて説明する。

【０１１１】

第１にＳ１００１において、サーバ装置８２０は情報処理端末８００からプログラム配布要求を受信する。

【0112】

次にＳ１００２において、Ｓ１００１で受信したプログラム配布要求に含まれる情報処理端末８００の端末ＩＤを取得する。

【0113】

Ｓ１００３において、固有情報配布履歴８４０に対してＳ１００２で取得した端末ＩＤを検索する。

【0114】

Ｓ１００４において、固有情報配布履歴８４０に同じ端末ＩＤが格納されているか否か判定する。

【0115】

固有情報配布履歴８４０に同じ端末ＩＤが格納されていた場合（Ｓ１００４でＹ）、情報処理端末８００へは既にプログラム固有情報８３５を配布済みであるため、Ｓ１００８においてプログラム８３３のみを送信し処理を終了する。

【0116】

固有情報配布履歴８４０に同じ端末ＩＤが格納されていない場合（Ｓ１００４でＮ）、Ｓ１００５において情報処理端末８００へは新たにプログラム固有情報８３５を割り当てる。

【0117】

次にＳ１００６において、Ｓ１００５で新たに割り当てたプログラム固有情報８３５に関し、端末ＩＤとプログラム固有情報ＩＤの対応を固有情報配布履歴８４０に追加する。

【0118】

Ｓ１００７において、プログラム固有情報８３５を情報処理端末８００に送信し、Ｓ１００８においてプログラム８３３を送信し処理を終了する。

【0119】

このようにサーバ装置８２０において固有情報配布履歴８４０を用いて配布管理することにより、１つの情報処理端末８００へ複数のプログラム固有情報８３５を配布することを防ぐ。これにより、プログラム固有情報８３５が含む情報を用いて不正端末と認識され、排除されている情報処理端末８００に対し、新たに

プログラム固有情報８３５を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

【０１２０】

なお、本実施の形態ではデータ格納部８０６とプログラム格納部８０５を別にしているが、同一の格納部としてもよい。また、本実施の形態で示した固有情報配布履歴８４０の形式は一例であり、最終配布日付情報を削除してもよいし、他の情報を付加してもよい。また、本実施の形態では固有情報配布履歴８４０に記載されている情報処理端末８００に対してプログラム固有情報８３５の配布を拒否しているが、その情報処理端末８００に対して既に配布済みのプログラム固有情報８３５を再度配布してもよい。また、本実施の形態では情報処理端末８００からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【０１２１】

（実施の形態４）

図１１に本発明の実施の形態４における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態３と異なる点は、サーバ装置１１２０がプログラム／固有情報対応表１１５０を保持する点である。

【０１２２】

プログラム／固有情報対応表１１５０は、プログラム固有情報を識別するプログラム固有情報ＩＤと、プログラム固有情報を使用するプログラムのプログラムＩＤとの対応を示した表である。

【０１２３】

本発明の実施の形態４における固有情報配布履歴１１４０と、プログラム／固有情報対応表１１５０の例を図１２に示す。

【０１２４】

固有情報配布履歴１２００は、プログラム固有情報１１３５を配布した情報処理端末１１００を識別するＩＤである端末ＩＤ１２０１、配布したプログラム固有情報１１３５が対応するプログラム１１３３を識別するＩＤであるプログラムＩＤ１２０２、配布したプログラム固有情報１１３５を識別するＩＤであるプロ

グラム固有情報ＩＤ１２０３を格納する。また、必要に応じてプログラム固有情報１１３５を最後に配布した日時を示す最終配布日付１２０４を格納する。本発明の実施の形態３における固有情報配布履歴と異なる点は、プログラム固有情報を使用するプログラムを識別するプログラムＩＤ１２０２が付加されている点である。

【０１２５】

図１２の例では、サーバ装置１１２０は情報処理端末１１００に５つのプログラム固有情報１１３５を配布済みであり、それぞれの端末ＩＤ１２０１、プログラムＩＤ１２０２、プログラム固有情報ＩＤ１２０３の組は、（端末ＩＤ、プログラムＩＤ、プログラム固有情報ＩＤ）＝（０００１、０００１、０００１）、（０００２、０００１、０００２）、（００１０、０００１、０００３）、（００１５、０００１、０００４）、（００２０、０００２、１００１）となる。

【０１２６】

またプログラム／固有情報対応表は、サーバ装置１１２０が管理しているプログラムのプログラムＩＤと、各プログラムが使用するプログラム固有情報を識別するプログラム固有情報ＩＤの対応関係を格納する。

【０１２７】

図１２の例では、サーバ装置１１２０はプログラムＩＤが０００１のプログラムを管理しており、そのプログラムが使用するプログラム固有情報としてプログラム固有情報ＩＤが０００１から１０００までのプログラム固有情報を管理している。同様にプログラムＩＤが０００２のプログラムと、そのプログラムが使用するプログラム固有情報ＩＤが１００１から２０００までのプログラム固有情報を管理している。また、プログラム／固有情報対応表は、プログラム固有情報をどこまで情報処理端末１１００に配布済みであり、次回のプログラム固有情報配布の際に、配布すべきプログラム固有情報を示す配布開始ＩＤ１２１３を格納する。

【０１２８】

図１２の例では、プログラムＩＤが０００１のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置１１２０は０１２３のプログラム固

有情報ＩＤを持つプログラム固有情報を割り当てることを示している。同様にプログラムＩＤが０００２のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置１１２０は１４２３のプログラム固有情報ＩＤを持つプログラム固有情報を割り当てることを示している。

【０１２９】

本発明の実施の形態４では、サーバ装置１１２０は、このプログラム／固有情報対応表を元に、情報処理端末１１００からのプログラムＩＤを指定したプログラム配布要求に対し、そのプログラムＩＤに対応したプログラム固有情報を配布する。

【０１３０】

本発明の実施の形態４におけるプログラム配布手順について、図１３を用いて説明する。

【０１３１】

第１にＳ１３０１において、サーバ装置１１２０は情報処理端末１１００からプログラム配布要求を受信する。

【０１３２】

次にＳ１３０２において、Ｓ１３０１で受信したプログラム配布要求に含まれる情報処理端末１１００の端末ＩＤ、プログラムＩＤを取得する。

【０１３３】

Ｓ１３０３において、固有情報配布履歴１１４０に対してＳ１３０２で取得した端末ＩＤ、プログラムＩＤを検索する。

【０１３４】

Ｓ１３０４において、固有情報配布履歴１１４０に同じ端末ＩＤかつ同じプログラムＩＤの履歴が格納されているか否か確認する。

【０１３５】

固有情報配布履歴１１４０に同じ端末ＩＤかつ同じプログラムＩＤの履歴が格納されていた場合（Ｓ１３０４でＹ）、情報処理端末１１００へは既に指定プログラムに対するプログラム固有情報１１３５を配布済みであるため、Ｓ１３０９においてプログラムのみを送信し処理を終了する。

【０１３６】

固有情報配布履歴１１４０に同じ端末ＩＤかつ同じプログラムＩＤの履歴が格納されていない場合（Ｓ１３０４でＮ）、Ｓ１３０５においてプログラム／固有情報対応表１１５０に格納されている配布開始ＩＤの情報を元に情報処理端末１１００へ新たにプログラム固有情報１１３５を割り当てる。

【０１３７】

次にＳ１３０６において、Ｓ１３０５で新たに割り当てたプログラム固有情報１１３５に関し、プログラム／固有情報対応表１１５０に格納されている配布開始ＩＤの値を更新する。

【０１３８】

また、Ｓ１３０７において、Ｓ１３０５で新たに割り当てたプログラム固有情報１１３５に関し、端末ＩＤとプログラム固有情報ＩＤの対応を固有情報配布履歴１１４０に追加する。

【０１３９】

Ｓ１３０８において、プログラム固有情報１１３５を情報処理端末１１００に送信し、Ｓ１３０９においてプログラム１１３３を送信し処理を終了する。

【０１４０】

このようにサーバ装置１１２０において固有情報配布履歴１１４０とプログラム／固有情報対応表１１５０を用いて配布管理することにより、１つの情報処理端末１１００で動作する同一プログラムに対して複数のプログラム固有情報１１３５を配布することを防ぐ。これにより、本発明の実施の形態３と同様に、プログラム固有情報１１３５が含む情報を用いて不正端末と認識され、排除されている情報処理端末１１００に対し、新たにプログラム固有情報１１３５を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

【０１４１】

また、本発明の本実施の形態４では、プログラム固有情報１１３５の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報１１３５の配布可否を判定することが可能となる。

【０１４２】

なお、本実施の形態ではデータ格納部１１０６とプログラム格納部１１０５を別にしているが、同一の格納部としてもよい。また、本実施の形態で示した固有情報配布履歴の形式は一例であり、最終配布日付情報を削除してもよいし、他の情報を付加してもよい。同様にプログラム／固有情報対応表の形式も一例であり、配布開始ＩＤを別の形式で管理してもよい。

【０１４３】

例えば、全プログラム固有情報ＩＤを格納したテーブルを持ち、各プログラム固有情報ＩＤに対して割り当て済みか否かを識別するフラグを設けることにより、プログラム固有情報１１３５の配布状態を管理してもよい。また、本実施の形態では固有情報配布履歴１１４０に記載されている情報処理端末１１００に対してプログラム固有情報１１３５の配布を拒否しているが、その情報処理端末１１００に対して既に配布済みのプログラム固有情報１１３５を再度配布してもよい。また、本実施の形態では情報処理端末１１００からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【０１４４】

（実施の形態５）

図１４に本発明の実施の形態５における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態１と異なる点は、サーバ装置１４２０がプログラム固有情報１４３５を情報処理端末１４００に配布した回数を管理するための配布回数情報１４４０を保持する点である。

【０１４５】

図１５に配布回数情報１４４０の情報格納例を示す。

【０１４６】

配布回数情報１５００は、プログラム固有情報１４３５を配布した情報処理端末１４００を識別するＩＤである端末ＩＤ１５０１、配布した回数を示す回数カウンタ１５０２を格納する。

【０１４７】

同図の例では、端末ＩＤが０００１、０００２の情報処理端末１４００に対し

てプログラム固有情報１４３５を１回配布しており、端末ＩＤが０００３の情報処理端末１４００に対してプログラム固有情報１４３５を配布していない。

【０１４８】

サーバ装置１４２０における配布回数情報１４４０を用いたプログラム配布手順について図１６を用いて説明する。

【０１４９】

第１にＳ1601において、サーバ装置１４２０は情報処理端末１４００からプログラム配布要求を受信する。

【０１５０】

次にＳ１６０２において、Ｓ１６０１で受信したプログラム配布要求に含まれる情報処理端末１４００の端末ＩＤを取得する。

【０１５１】

Ｓ１６０３において、配布回数情報１４４０に対してＳ１６０２で取得した端末ＩＤを検索し、回数カウンタの値を取得する。

【０１５２】

Ｓ１６０４において、取得した回数カウンタの値が規定値以上か否かを判定する。

【０１５３】

取得した回数カウンタの値が規定値以上であった場合（Ｓ１６０４でＹ）、情報処理端末１４００へは既にプログラム固有情報１４３５を規定回数以上配布しているため、Ｓ１６０８においてプログラム１４３３のみを送信し処理を終了する。

【０１５４】

取得した回数カウンタの値が規定値未満であった場合（Ｓ１６０４でＮ）、Ｓ１６０５において情報処理端末１４００へは新たにプログラム固有情報１４３５を割り当てる。

【０１５５】

次にＳ１６０６において、配布回数情報１４４０内に格納されている回数カウンタの値を加算する。

【０１５６】

Ｓ１６０７において、プログラム固有情報１４３５を情報処理端末１４００に送信し、Ｓ１６０８においてプログラム１４３３を送信し処理を終了する。

【０１５７】

このようにサーバ装置１４２０において配布回数情報１４４０を用いて配布管理することにより、１つの情報処理端末１４００へ規定数以上のプログラム固有情報１４３５を配布することを防ぐ。特に規定値を１に設定した場合、本発明の実施の形態３と同様、プログラム固有情報１４３５が含む情報を用いて不正端末と認識され、排除されている情報処理端末１４００に対し、新たにプログラム固有情報１４３５を割り当てることにより、不正端末が排除を回避することを防ぐことが可能となる。

【０１５８】

なお、本実施の形態ではデータ格納部１４０６とプログラム格納部１４０５を別にしているが、同一の格納部としてもよい。また、本実施の形態で示した配布回数情報の形式は一例であり、他の情報を付加してもよい。また、本実施の形態では情報処理端末１４００からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【０１５９】

（実施の形態６）

図１７に本発明の実施の形態６における情報処理端末とサーバ装置の構成図を示す。同図において、本発明の実施の形態５と異なる点は、サーバ装置１７２０がプログラム／固有情報対応表１７５０を保持する点である。

【０１６０】

プログラム／固有情報対応表１７５０は、プログラム固有情報を識別するプログラム固有情報ＩＤと、プログラム固有情報を使用するプログラムのプログラムＩＤとの対応を示した表である。

【０１６１】

本発明の実施の形態６における配布回数情報１７４０と、プログラム／固有情

報対応表１７５０の例を図１８に示す。

【０１６２】

配布回数情報１８００は、配布したプログラム固有情報１７３５が対応するプログラム１７３３を識別するＩＤであるプログラムＩＤ１８０１、プログラム固有情報１７３５を配布した情報処理端末１７００を識別するＩＤである端末ＩＤ１８０２、配布した回数を示す回数カウンタ１８０３を格納する。本発明の実施の形態５における配布回数情報と異なる点は、プログラム固有情報を使用するプログラムを識別するプログラムＩＤが付加されている点である。

【０１６３】

図１８の例では、プログラムＩＤが０００１のプログラムが使用するプログラム固有情報１７３５を、端末ＩＤが０００１、０００２の情報処理端末１７００に対して１回配布しており、端末ＩＤが０００３の情報処理端末１７００に対してプログラム固有情報１７３５を配布していない。また同様に、プログラムＩＤが０００２のプログラムが使用するプログラム固有情報１７３５を、端末ＩＤが０００１の情報処理端末１７００に対して１回配布しており、端末ＩＤが０００２、０００３の情報処理端末１７００に対してプログラム固有情報１７３５を配布していない。

【０１６４】

またプログラム／固有情報対応表１７５０は、サーバ装置１７２０が管理しているプログラムのプログラムＩＤと、各プログラムが使用するプログラム固有情報を識別するプログラム固有情報ＩＤの対応関係を格納する。図１８の例では、サーバ装置１７２０はプログラムＩＤが０００１のプログラムを管理しており、そのプログラムが使用するプログラム固有情報としてプログラム固有情報ＩＤが０００１から１０００までのプログラム固有情報を管理している。同様にプログラムＩＤが０００２のプログラムと、そのプログラムが使用するプログラム固有情報ＩＤが１００１から２０００までのプログラム固有情報を管理している。

【０１６５】

また、プログラム／固有情報対応表１７５０は、プログラム固有情報１７３５をどこまで情報処理端末１７００に配布済みであり、次回のプログラム固有情報

配布の際に、配布すべきプログラム固有情報１７３５を示す配布開始ＩＤ１８１３を格納する。図１８の例では、プログラムＩＤが０００１のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置１７２０は０１２３のプログラム固有情報ＩＤを持つプログラム固有情報を割り当てることを示している。同様にプログラムＩＤが０００２のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置１７２０は１４２３のプログラム固有情報ＩＤを持つプログラム固有情報を割り当てることを示している。

【０１６６】

本発明の実施の形態６では、サーバ装置１７２０は、このプログラム／固有情報対応表１７５０を元に、情報処理端末１７００からのプログラムＩＤを指定したプログラム配布要求に対し、そのプログラムＩＤに対応したプログラム固有情報１７３５を配布する。

【０１６７】

本発明の実施の形態６におけるプログラム配布手順について、図１９を用いて説明する。

【０１６８】

第１にＳ１９０１において、サーバ装置１７２０は情報処理端末１７００からプログラム配布要求を受信する。

【０１６９】

次にＳ１９０２において、Ｓ１９０１で受信したプログラム配布要求に含まれる情報処理端末１７００の端末ＩＤ、プログラムＩＤを取得する。

【０１７０】

Ｓ１９０３において、配布回数情報１７４０に対してＳ１９０２で取得した端末ＩＤ、プログラムＩＤを検索し、回数カウンタの値を取得する。

【０１７１】

Ｓ１９０４において、取得した回数カウンタの値が規定値以上か否かを判定する。

【０１７２】

取得した回数カウンタの値が規定値以上であった場合（Ｓ１９０４でＹ）、情

報処理端末１７００へは既にプログラム固有情報１７３５を規定回数以上配布しているため、Ｓ１９０９においてプログラム１７３３のみを送信し処理を終了する。

【０１７３】

取得した回数カウンタの値が規定値未満であった場合（Ｓ１９０４でＮ）、Ｓ１９０５においてプログラム／固有情報対応表１７５０に格納されている配布開始ＩＤの情報を元に情報処理端末１７００へ新たにプログラム固有情報１７３５を割り当てる。

【０１７４】

次にＳ１９０６において、Ｓ１９０５で新たに割り当てたプログラム固有情報１７３５に関し、プログラム／固有情報対応表１７５０に格納されている配布開始ＩＤの値を更新する。

【０１７５】

また、Ｓ１９０７において、配布回数情報１７４０内に格納されている回数カウンタの値を加算する。

【０１７６】

Ｓ１９０８において、プログラム固有情報１７３５を情報処理端末１７００に送信し、Ｓ１９０９においてプログラム１７３３を送信し処理を終了する。

【０１７７】

このようにサーバ装置１７２０において配布回数情報１７４０とプログラム／固有情報対応表１７５０を用いて配布管理することにより、１つの情報処理端末１７００で動作する同一プログラムに対して規定数以上のプログラム固有情報１７３５を配布することを防ぐ。これにより、本発明の実施の形態５と同様に、プログラム固有情報１７３５の配布回数を制限することが可能となる。

【０１７８】

また、本発明の本実施の形態６では、プログラム固有情報の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報の配布可否を判定することが可能となる。

【０１７９】

なお、本実施の形態ではデータ格納部とプログラム格納部を別にしているが、同一の格納部としてもよい。また、本実施の形態で示した配布回数情報の形式は一例であり、他の情報を付加してもよい。同様にプログラム／固有情報対応表の形式も一例であり、配布開始ＩＤを別の形式で管理してもよい。また、本実施の形態では情報処理端末からの要求はプログラム配布要求であり、プログラムの配布が伴うが、プログラム固有情報配布要求とし、プログラムの配布を伴わない形態としてもよい。

【０１８０】

【発明の効果】

以上のように、情報処理端末を一意に識別する端末ＩＤと、情報処理端末毎に異なる固有鍵を外部から書き換えが行えない不揮発性メモリに格納する情報処理端末と、情報処理端末で動作するプログラム、プログラムに関する情報を格納したプログラムヘッダ、プログラムが使用する固有の情報であるプログラム固有情報、プログラム固有情報に関する情報を格納した固有情報ヘッダを保持するサーバ装置において、情報処理端末の端末ＩＤを含んだプログラム配布要求に対し、それぞれ電子的な署名が付加されたプログラム、プログラムヘッダ、プログラム固有情報、固有情報ヘッダを配布し、情報処理端末内でプログラムを固有鍵で再暗号化し格納することで、配布後のプログラムを不正改ざんから守ることができる。

【０１８１】

また、プログラムヘッダにプログラムを一意に特定することが可能な認証子を含み、固有情報ヘッダにプログラム固有情報を一意に特定することが可能な認証子を含み、プログラムヘッダと固有情報ヘッダに電子的な署名を付加することで、全ての情報の署名を付加することなく、情報の正当性検証を行うことができる。

【０１８２】

また、プログラム固有情報を配布した情報処理端末の端末ＩＤと、情報処理端末に配布したプログラム固有情報のプログラム固有情報ＩＤの対応を管理する固有情報配布履歴をサーバ装置に保持し、複数のプログラム固有情報を１つの情報

処理端末に割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【０１８３】

また、プログラム固有情報のプログラム固有情報ＩＤと、プログラムのプログラムＩＤの対応を示すプログラム／固有情報対応表と、固有情報配布履歴をサーバ装置に保持し、複数のプログラム固有情報を、情報処理端末で実行される１つのプログラムに割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【０１８４】

また、プログラム固有情報を配布した情報処理端末の端末ＩＤと、プログラム固有情報を配布した回数を示す配布回数情報をサーバ装置に保持し、規定数以上のプログラム固有情報を１つの情報処理端末に割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【０１８５】

また、プログラム固有情報のプログラム固有情報ＩＤと、プログラムのプログラムＩＤの対応を示すプログラム／固有情報対応表と、配布回数情報をサーバ装置に保持し、規定数以上のプログラム固有情報を、情報処理端末で実行される１つのプログラムに割り当てることを防ぐことで、不正端末を排除する仕組みに対し、不正端末が排除を回避することを防ぐことができる。

【図面の簡単な説明】

【図１】

署名を用いたプログラム正当性検証方法の例を示す図

【図２】

本発明の実施の形態１における情報処理端末とサーバ装置の構成を示す図

【図３】

本発明の実施の形態１におけるプログラムヘッダとプログラムの関係を示す図

【図４】

本発明の実施の形態１における固有情報ヘッダとプログラム固有情報の関係を

示す図

【図５】

プログラム更新手順の例を示す図

【図６】

本発明の実施の形態２におけるプログラムヘッダとプログラムの関係を示す図

【図７】

本発明の実施の形態２における固有情報ヘッダとプログラム固有情報の関係を示す図

【図８】

本発明の実施の形態３における情報処理端末とサーバ装置の構成を示す図

【図９】

本発明の実施の形態３における固有情報配布履歴の構成を示す図

【図１０】

本発明の実施の形態３における固有情報配布履歴を用いたプログラム配布手順を示すフローチャート

【図１１】

本発明の実施の形態４における情報処理端末とサーバ装置の構成を示す図

【図１２】

本発明の実施の形態４における固有情報配布履歴、プログラム／固有情報対応表の構成を示す図

【図１３】

本発明の実施の形態４における固有情報配布履歴、プログラム／固有情報対応表を用いたプログラム配布手順を示すフローチャート

【図１４】

本発明の実施の形態５における情報処理端末とサーバ装置の構成を示す図

【図１５】

本発明の実施の形態５における配布回数情報の構成を示す図

【図１６】

本発明の実施の形態５における配布回数情報を用いたプログラム配布手順を示

すフローチャート

【図１７】

本発明の実施の形態６における情報処理端末とサーバ装置の構成を示す図

【図１８】

本発明の実施の形態６における配布回数情報、プログラム／固有情報対応表の構成を示す図

【図１９】

本発明の実施の形態６における配布回数情報、プログラム／固有情報対応表を用いたプログラム配布手順を示すフローチャート

【符号の説明】

１００　プログラム発行者

１１０　ＣＡ

１２０　ユーザ

１０１，１１１　公開鍵

１０２，１１２　秘密鍵

１０３　プログラム発行者公開鍵証明書

１０４　署名付きプログラム

１２１，２１６，２３３，３１０，６１０，８３３，１１３３，１４３３，１７３３　プログラム

２００，８００，１１００，１４００，１７００　情報処理端末

２０１，２２１，８０１，８２１，１１０１，１１２１，１４０１，１４２１，１７０１，１７２１　ＣＰＵ

２０２，２２２，８０２，８２２，１１０２，１１２２，１４０２，１４２２，１７０２，１７２２　ＡＭ

２０３，２２３，８０３，８２３，１１０３，１１２３，１４０３，１４２３，１７０３，１７２３　暗号処理部

２０４，２２４，８０４，８２４，１１０４，１１２４，１４０４，１４２４，１７０４，１７２４　通信処理部

２０５，８０５，１１０５，１４０５，１７０５　プログラム格納部

２０６，２２５，８０６，８２５，１１０６，１１２５，１４０６，１４２５，１７０６，１７２５　データ格納部

２０７，８０７，１１０７，１４０７，１７０７　秘匿情報格納部

２０８　プログラム管理情報

２０９，２２９，８２９，１１２９，１４２９，１７２９　ＣＡ公開鍵

２１０　端末固有鍵

２１１　端末秘密鍵

２１２　プログラム固有情報

２１３　端末公開鍵証明書

２１４，９０１，１２０１，１５０１，１８０２　端末ＩＤ

２１５，２３１，３０５，３１１，４０６，４２２，６０５，７０７，８３１，１１３１，１４３１，１７３１　ＣＡ署名

２２０，８２０，１１２０，１４２０，１７２０　サーバ装置

２２６，８２６，１１２６，１４２６，１７２６　配布情報格納部

２２７，８２７，１１２７，１４２７，１７２７　サーバ秘密鍵

２２８，８２８，１１２８，１４２８，１７２８　サーバ公開鍵証明書

２３０，８３０，１１３０，１４３０，１７３０　サーバＩＤ

２３２，３００，６００，８３２，１１３２，１４３２，１７３２　プログラムヘッダ

２３４，４００，７００，８３４，１１３４，１４３４，１７３４　固有情報ヘッダ

２３５，４２０，４２１，７２０，７２１，８３５，１１３５，１４３５，１７３５　プログラム固有情報

３０１，４０２，６０１，７０２，１２０２，１２１１，１８０１，１８１１　プログラムＩＤ

３０２，６０２　バージョン番号

３０３，６０３　プログラムサイズ

３０４，６０４　プログラムハッシュ値

４０１，７０１，９０２，１２０３，１２１２，１８１２　プログラム固有情

報ＩＤ

４０３，７０３　固有情報数

４０４，７０４　全体サイズ

４０５，７０６　固有情報サブヘッダ

４１１，７１１　プログラム固有情報サブＩＤ

４１２，７１２　サイズ

７０５　プログラム固有情報ハッシュ値

８４０，９００，１１４０，１２００　固有情報配布履歴

９０３，１２０４　最終配布日付

１１５０，１２１０，１７５０，１８１０　プログラム／固有情報対応表

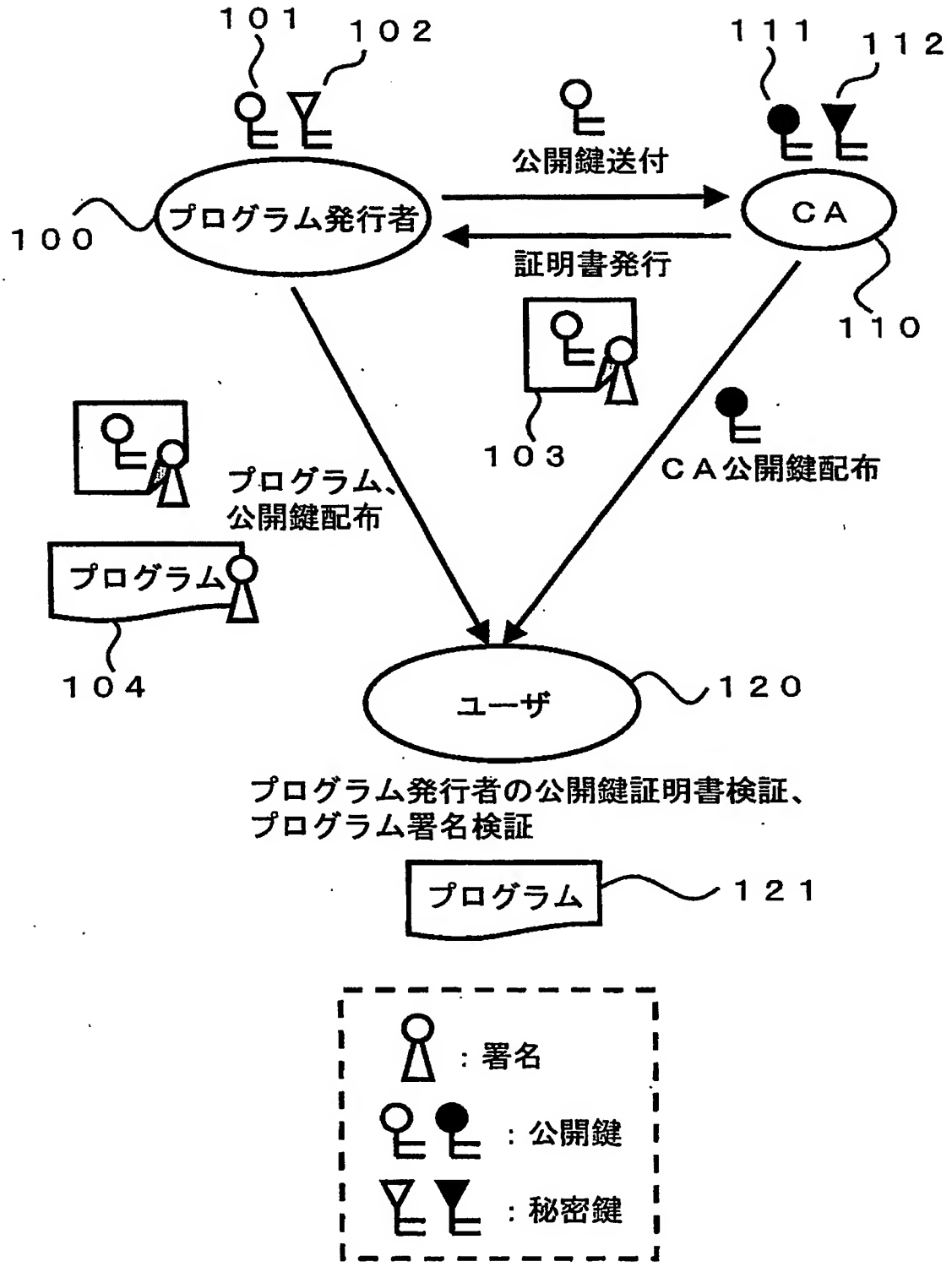
１２１３，１８１３　配布開始ＩＤ

１４４０，１５００，１７４０，１８００　配布回数情報

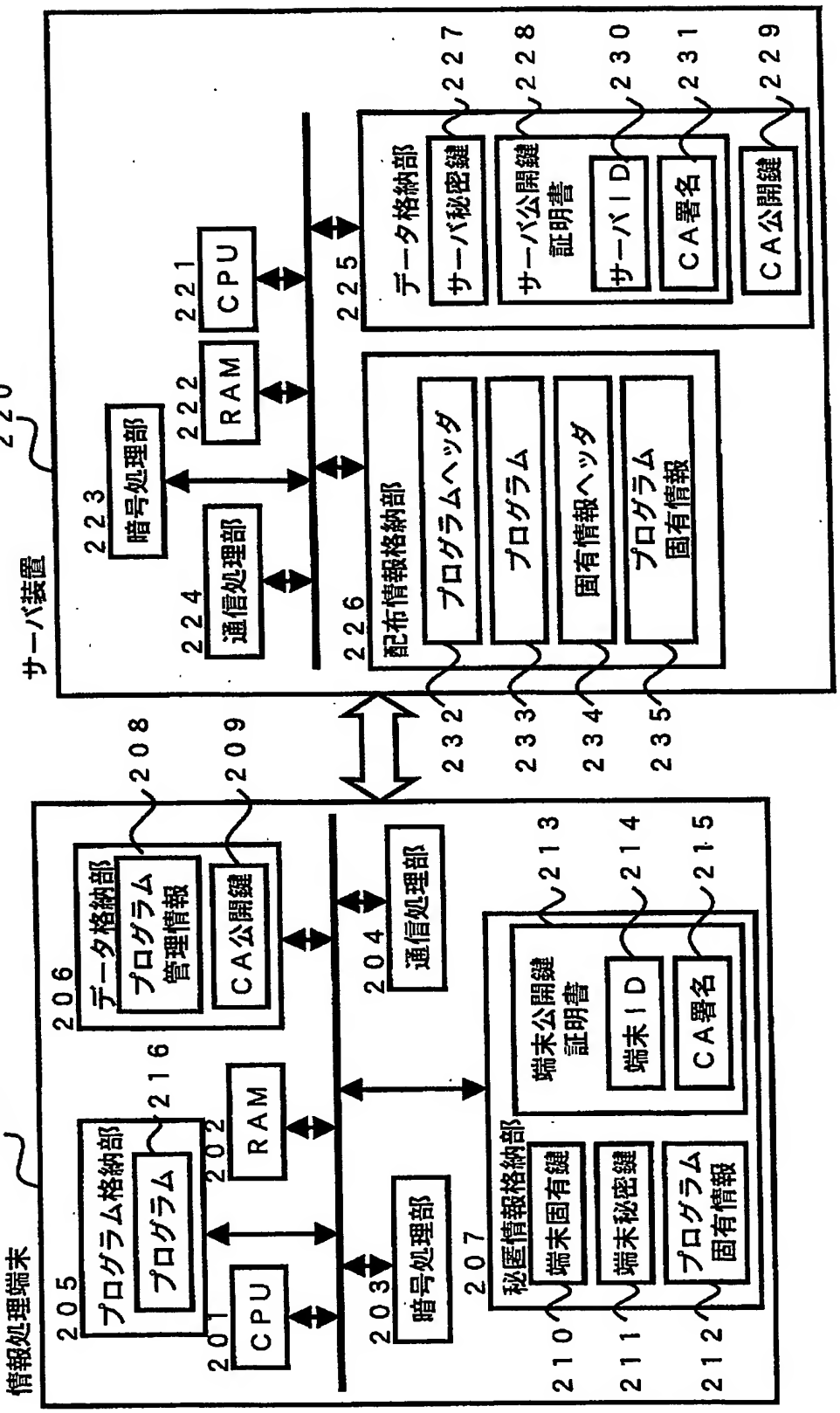
１５０２，１８０３　回数カウンタ

【書類名】　　図面

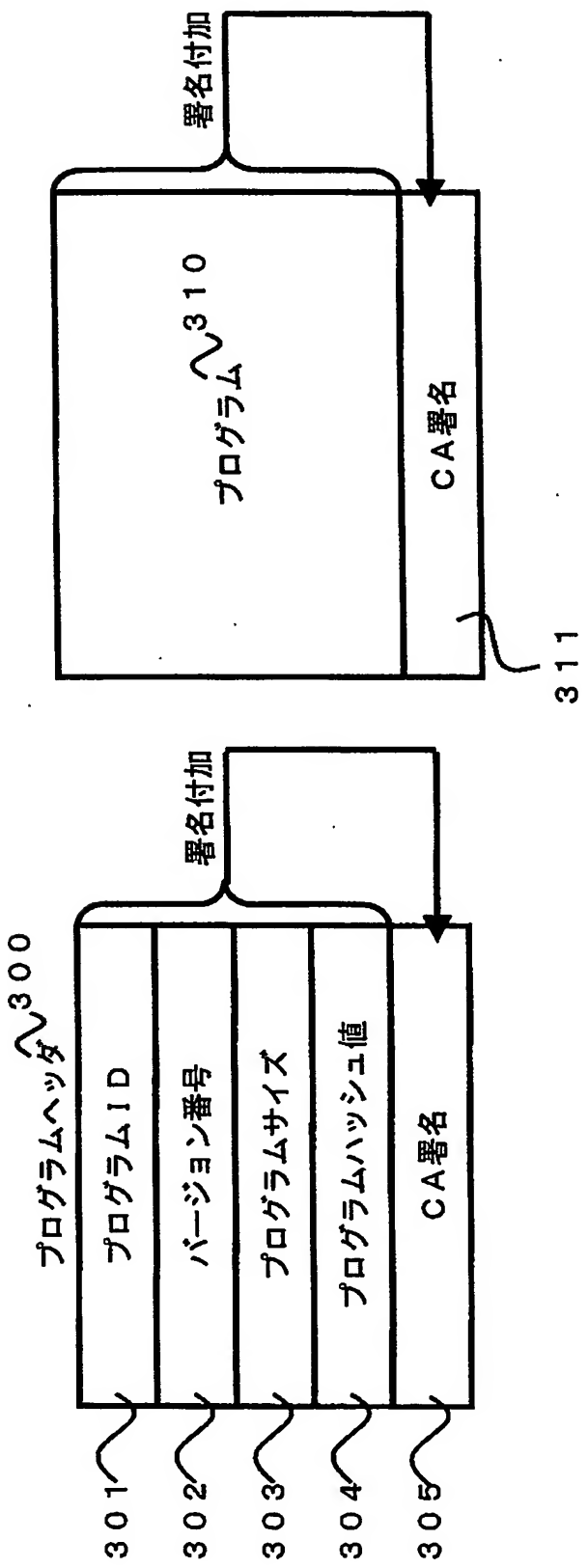
【図１】


１０１
１０２
１１１
１１２
公開鍵送付
プログラム発行者
１００
ＣＡ
証明書発行
１１０
１０３
ＣＡ公開鍵配布
プログラム、
公開鍵配布
プログラム
１０４
ユーザ
１２０
プログラム発行者の公開鍵証明書検証、
プログラム署名検証
プログラム
１２１
：署名
：公開鍵
：秘密鍵

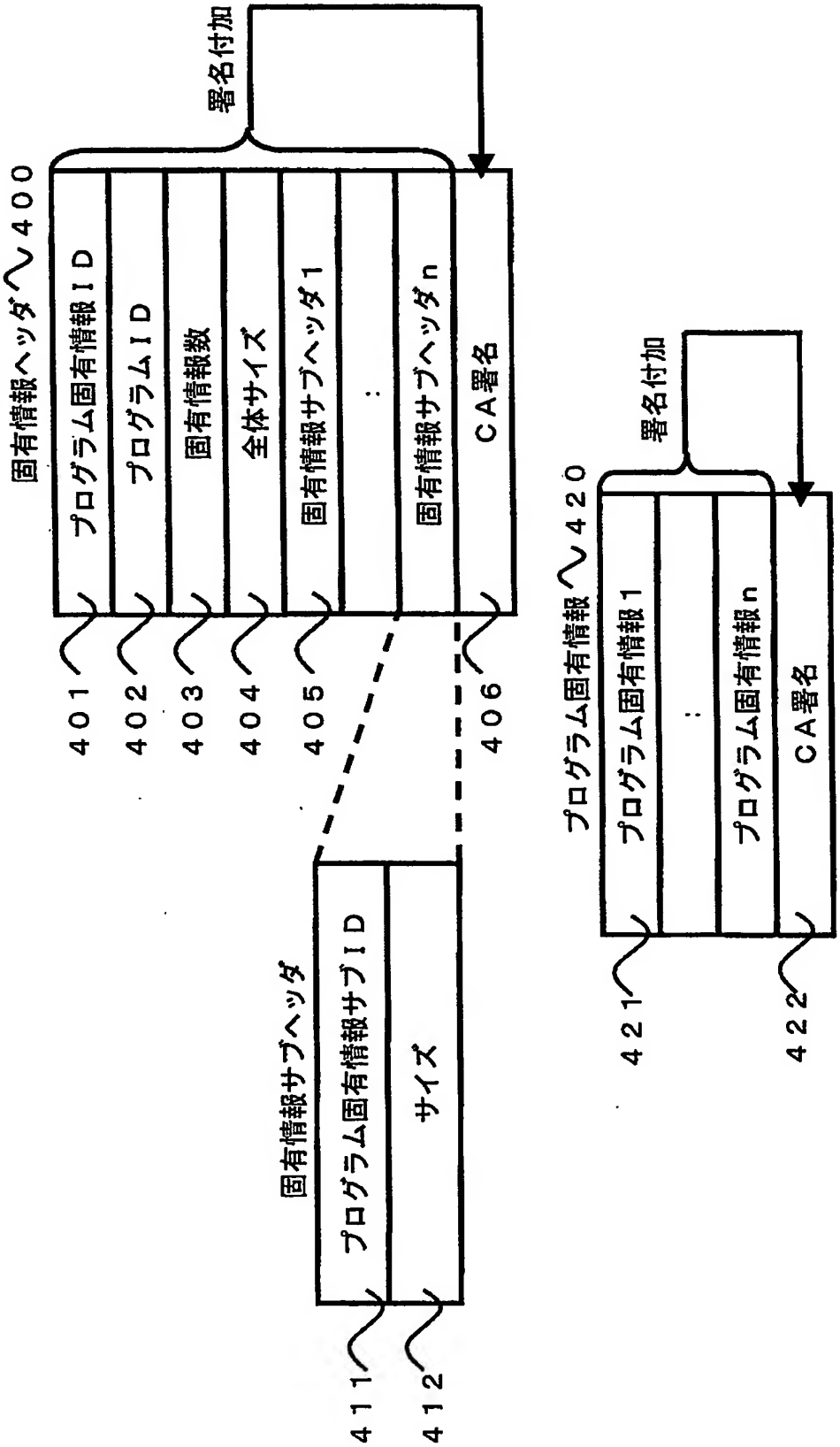
【図２】


情報処理端末
200
CPU
201
RAM
202
暗号処理部
203
通信処理部
204
プログラム格納部
205
プログラム
216
データ格納部
206
プログラム管理情報
CA公開鍵
208
209
秘匿情報格納部
207
端末固有鍵
端末秘密鍵
プログラム固有情報
210
211
212
端末公開鍵証明書
端末ID
CA署名
213
214
215
サーバ装置
220
CPU
221
RAM
222
暗号処理部
223
通信処理部
224
データ格納部
225
サーバ秘密鍵
サーバ公開鍵証明書
サーバID
CA署名
CA公開鍵
227
228
230
231
229
配布情報格納部
226
プログラムヘッダ
プログラム
固有情報ヘッダ
プログラム固有情報
232
233
234
235

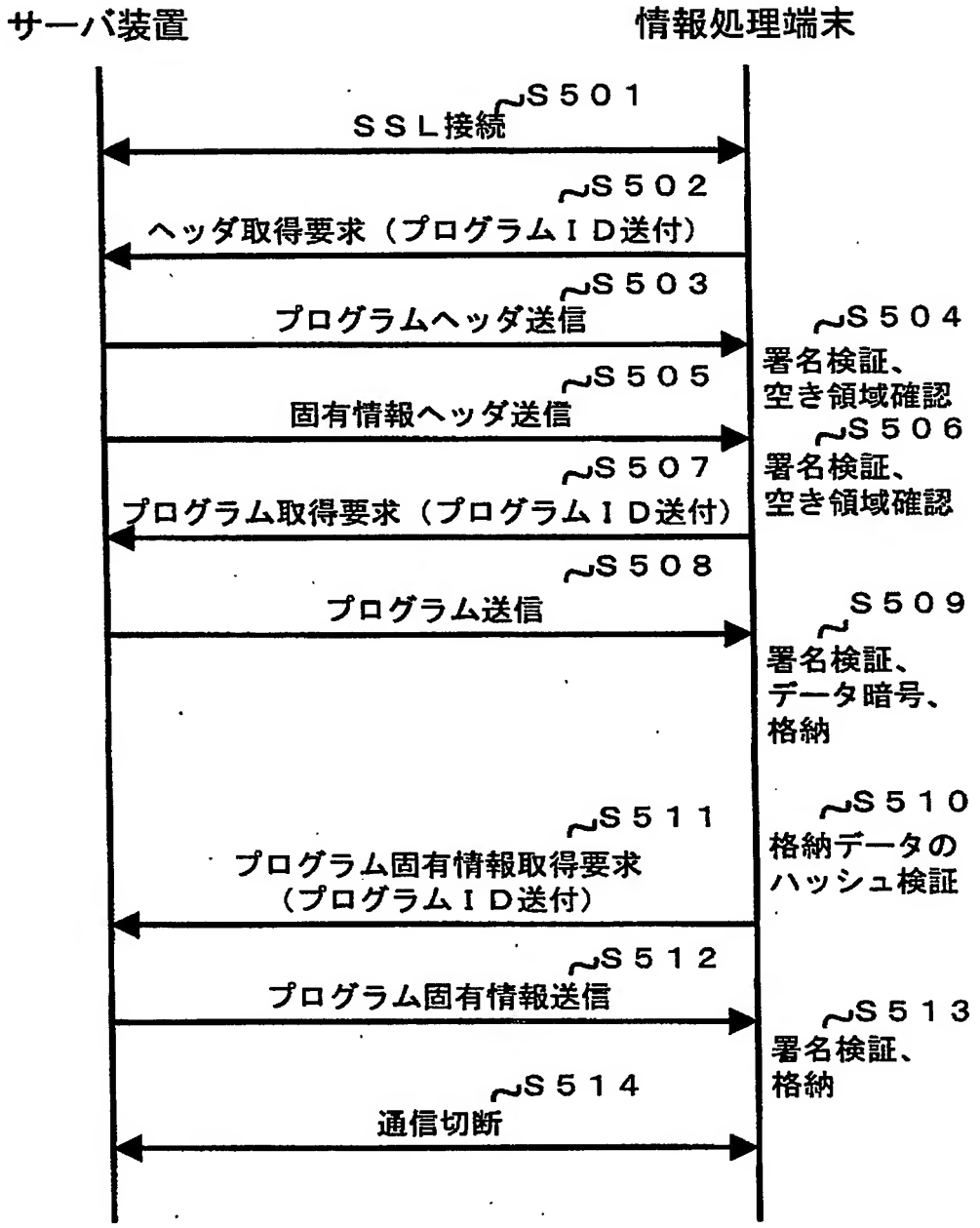
【図３】


署名付加
プログラム
310
CA署名
311
署名付加
プログラムヘッダ
300
プログラムＩＤ
バージョン番号
プログラムサイズ
プログラムハッシュ値
CA署名
301
302
303
304
305

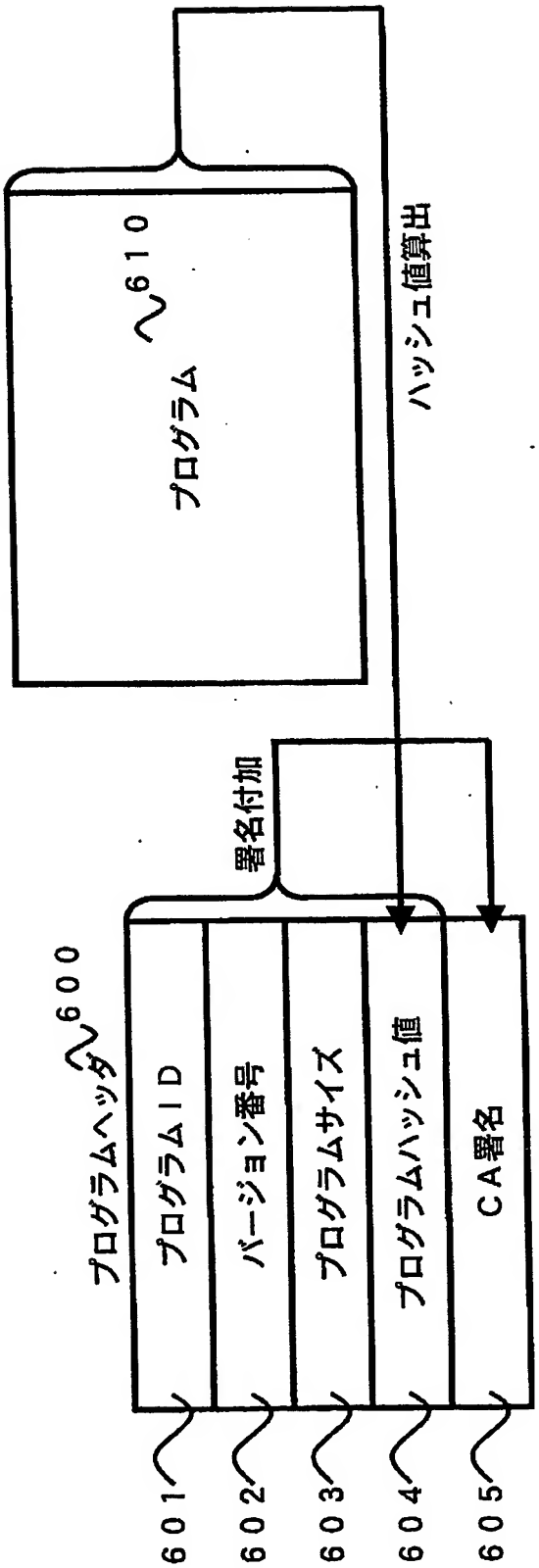
【図４】


署名付加
固有情報ヘッダ
４００
プログラム固有情報ＩＤ
プログラムＩＤ
固有情報数
全体サイズ
固有情報サブヘッダ１
固有情報サブヘッダｎ
ＣＡ署名
４０１
４０２
４０３
４０４
４０５
４０６
固有情報サブヘッダ
プログラム固有情報サブＩＤ
サイズ
４１１
４１２
署名付加
プログラム固有情報
４２０
プログラム固有情報１
プログラム固有情報ｎ
ＣＡ署名
４２１
４２２

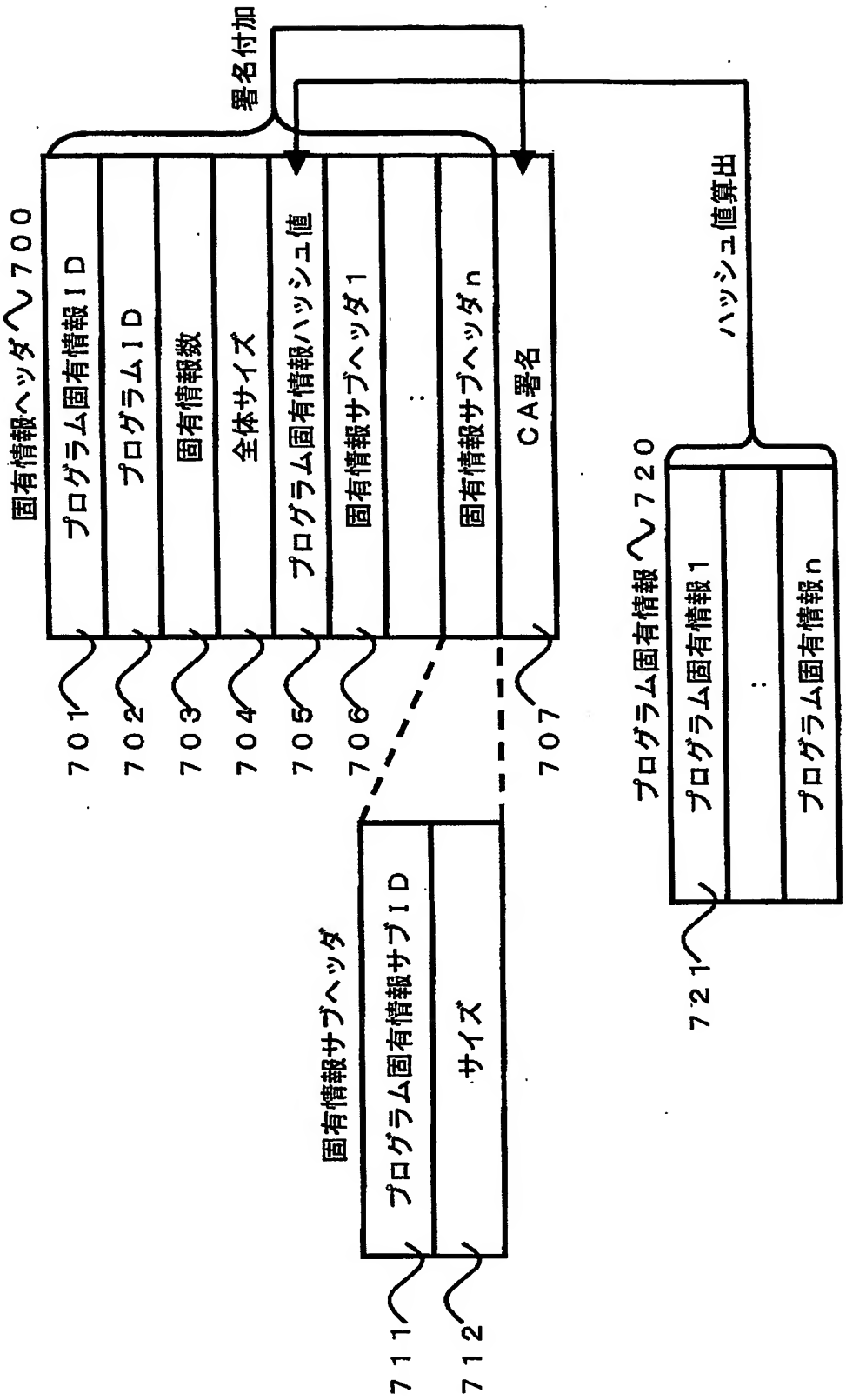
【図５】


サーバ装置
情報処理端末
S５０１
ＳＳＬ接続
S５０２
ヘッダ取得要求（プログラムＩＤ送付）
S５０３
プログラムヘッダ送信
S５０４
署名検証、
空き領域確認
S５０５
固有情報ヘッダ送信
S５０６
署名検証、
空き領域確認
S５０７
プログラム取得要求（プログラムＩＤ送付）
S５０８
プログラム送信
S５０９
署名検証、
データ暗号、
格納
S５１０
格納データの
ハッシュ検証
S５１１
プログラム固有情報取得要求
（プログラムＩＤ送付）
S５１２
プログラム固有情報送信
S５１３
署名検証、
格納
S５１４
通信切断

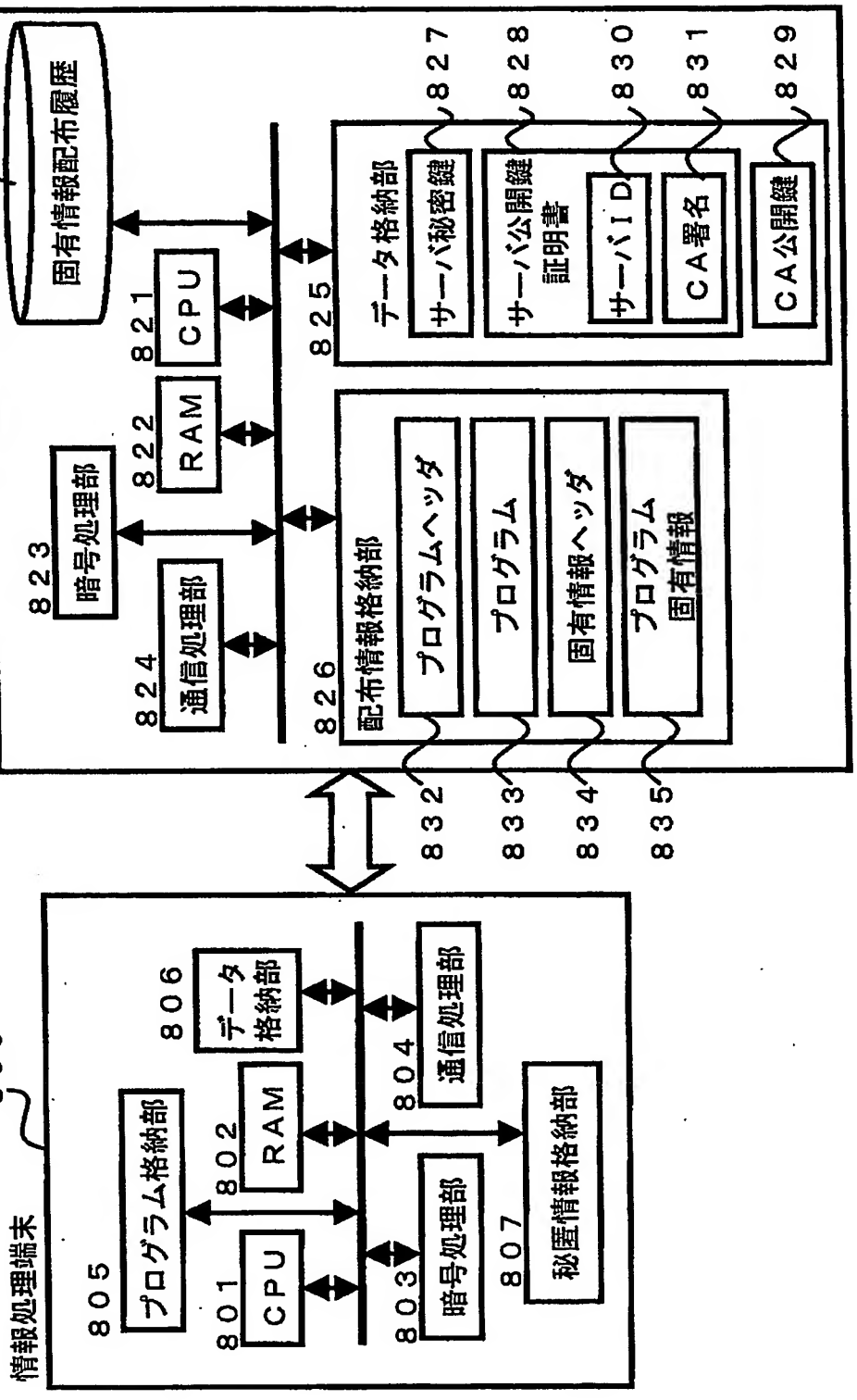
【図６】


プログラム
610
ハッシュ値算出
署名付加
プログラムヘッダ
600
プログラムＩＤ
バージョン番号
プログラムサイズ
プログラムハッシュ値
ＣＡ署名
601
602
603
604
605

【図７】


固有情報ヘッダ700
プログラム固有情報ＩＤ
プログラムＩＤ
固有情報数
全体サイズ
プログラム固有情報ハッシュ値
固有情報サブヘッダ１
固有情報サブヘッダｎ
ＣＡ署名
署名付加
701
702
703
704
705
706
707
固有情報サブヘッダ
プログラム固有情報サブＩＤ
サイズ
711
712
プログラム固有情報720
プログラム固有情報１
プログラム固有情報ｎ
721
ハッシュ値算出

【図８】

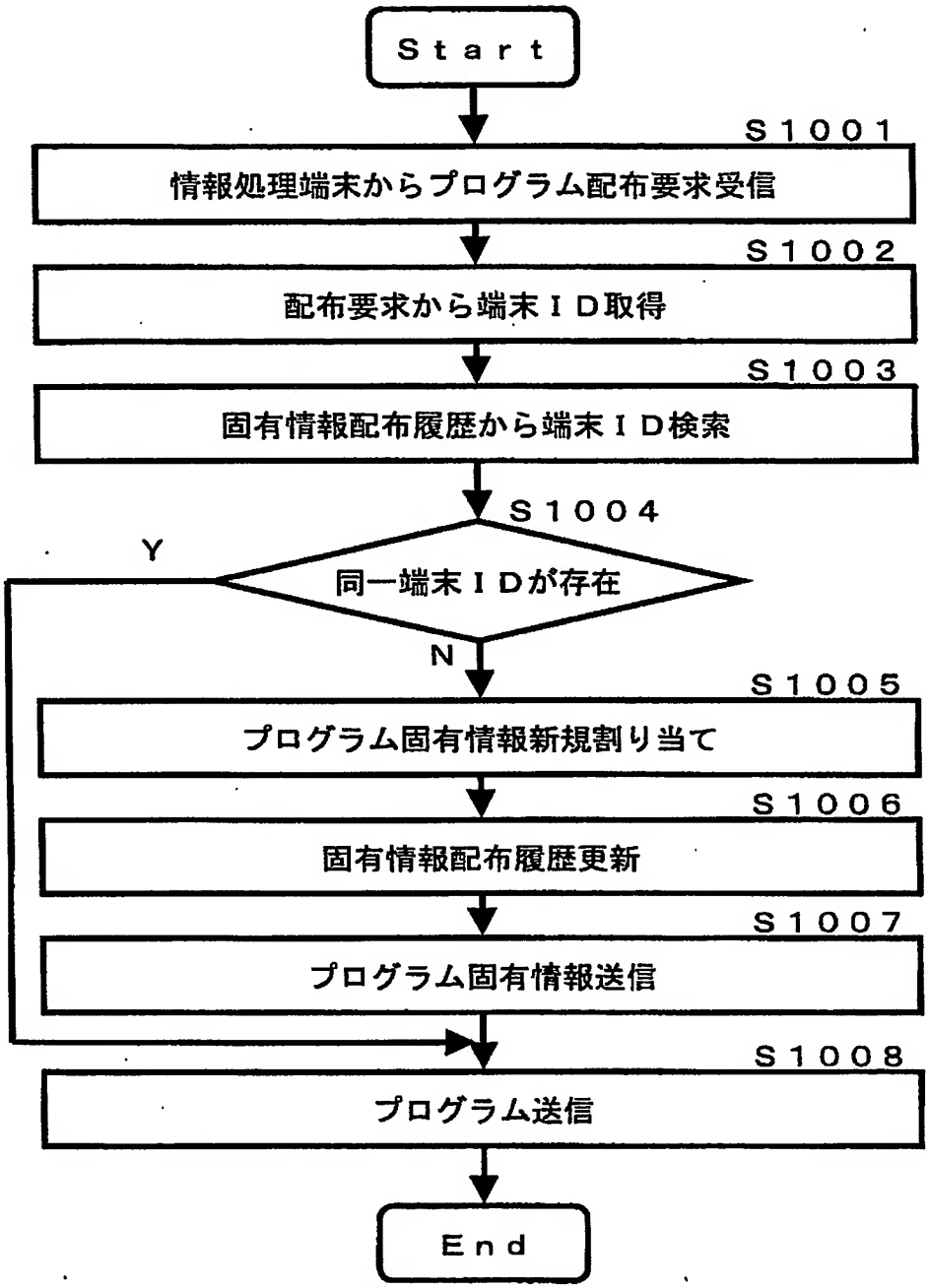

情報処理端末
800
CPU
801
RAM
802
暗号処理部
803
通信処理部
804
秘匿情報格納部
807
データ格納部
806
プログラム格納部
805
サーバ装置
820
CPU
821
RAM
822
暗号処理部
823
通信処理部
824
固有情報配布履歴
840
データ格納部
825
サーバ秘密鍵
827
サーバ公開鍵証明書
828
サーバＩＤ
830
ＣＡ署名
831
ＣＡ公開鍵
829
配布情報格納部
826
プログラムヘッダ
832
プログラム
833
固有情報ヘッダ
834
プログラム固有情報
835

【図９】

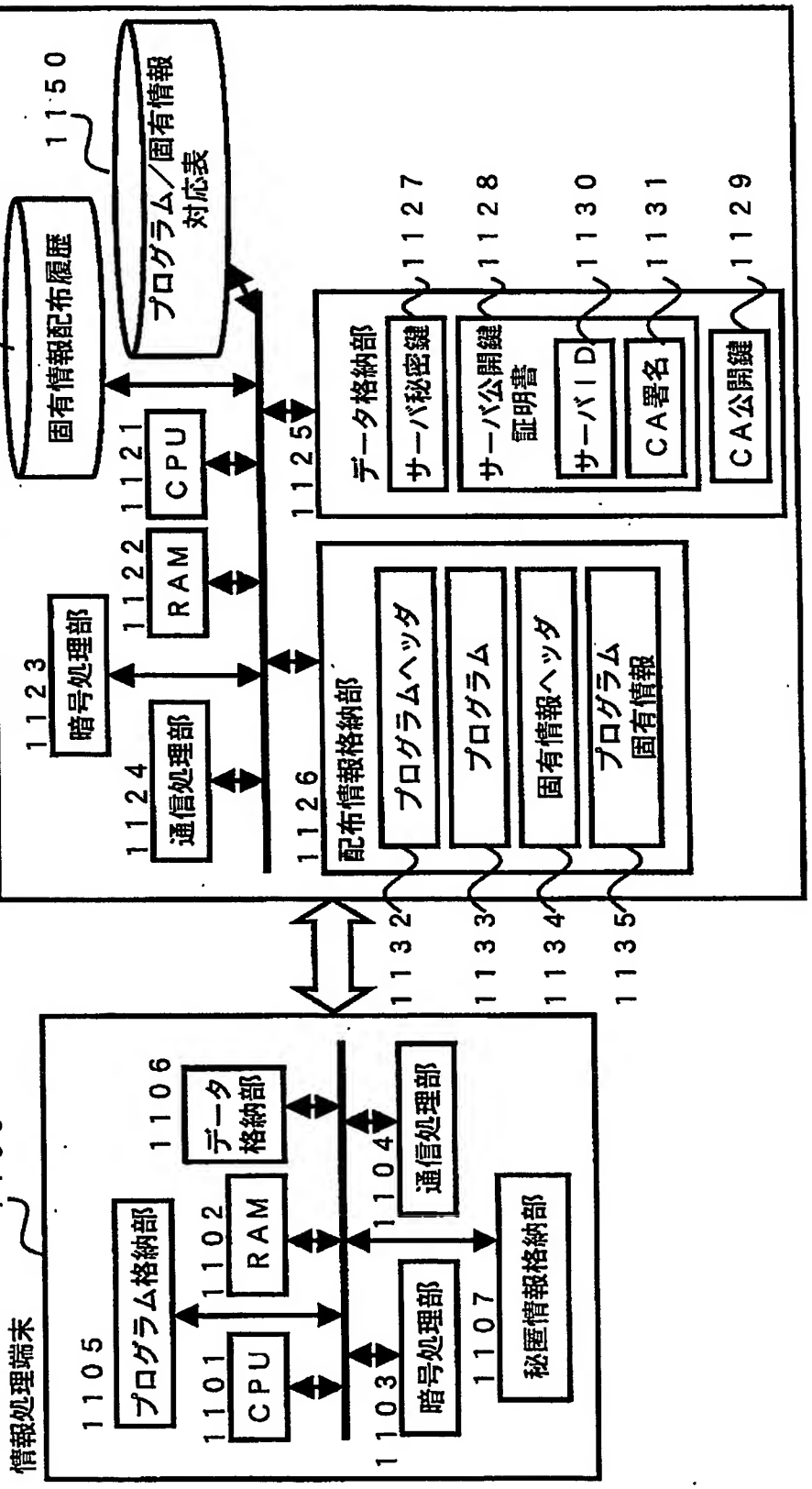
固有情報配布履歴 900

端末ＩＤ (901)	プログラム固有情報ＩＤ (902)	最終配布日付 (903)
０００１	０００１	２００２．３．１２
０００２	０００２	２００２．３．１２
００１０	０００３	２００２．３．１３
００１５	０００４	２００２．３．１４
００２０	０００５	２００２．３．１４

【図１０】


Ｓｔａｒｔ
Ｓ１００１
情報処理端末からプログラム配布要求受信
Ｓ１００２
配布要求から端末ＩＤ取得
Ｓ１００３
固有情報配布履歴から端末ＩＤ検索
Ｓ１００４
Ｙ
同一端末ＩＤが存在
Ｎ
Ｓ１００５
プログラム固有情報新規割り当て
Ｓ１００６
固有情報配布履歴更新
Ｓ１００７
プログラム固有情報送信
Ｓ１００８
プログラム送信
Ｅｎｄ

【図１１】


情報処理端末
1100
CPU
1101
RAM
1102
暗号処理部
1103
通信処理部
1104
プログラム格納部
1105
データ格納部
1106
秘匿情報格納部
1107
サーバ装置
1120
CPU
1121
RAM
1122
暗号処理部
1123
通信処理部
1124
配布情報格納部
1126
データ格納部
1125
固有情報配布履歴
1140
プログラム／固有情報対応表
1150
プログラムヘッダ
1132
プログラム
1133
固有情報ヘッダ
1134
プログラム固有情報
1135
サーバ秘密鍵
1127
サーバ公開鍵証明書
1128
サーバＩＤ
1130
ＣＡ署名
1131
ＣＡ公開鍵
1129

【図１２】

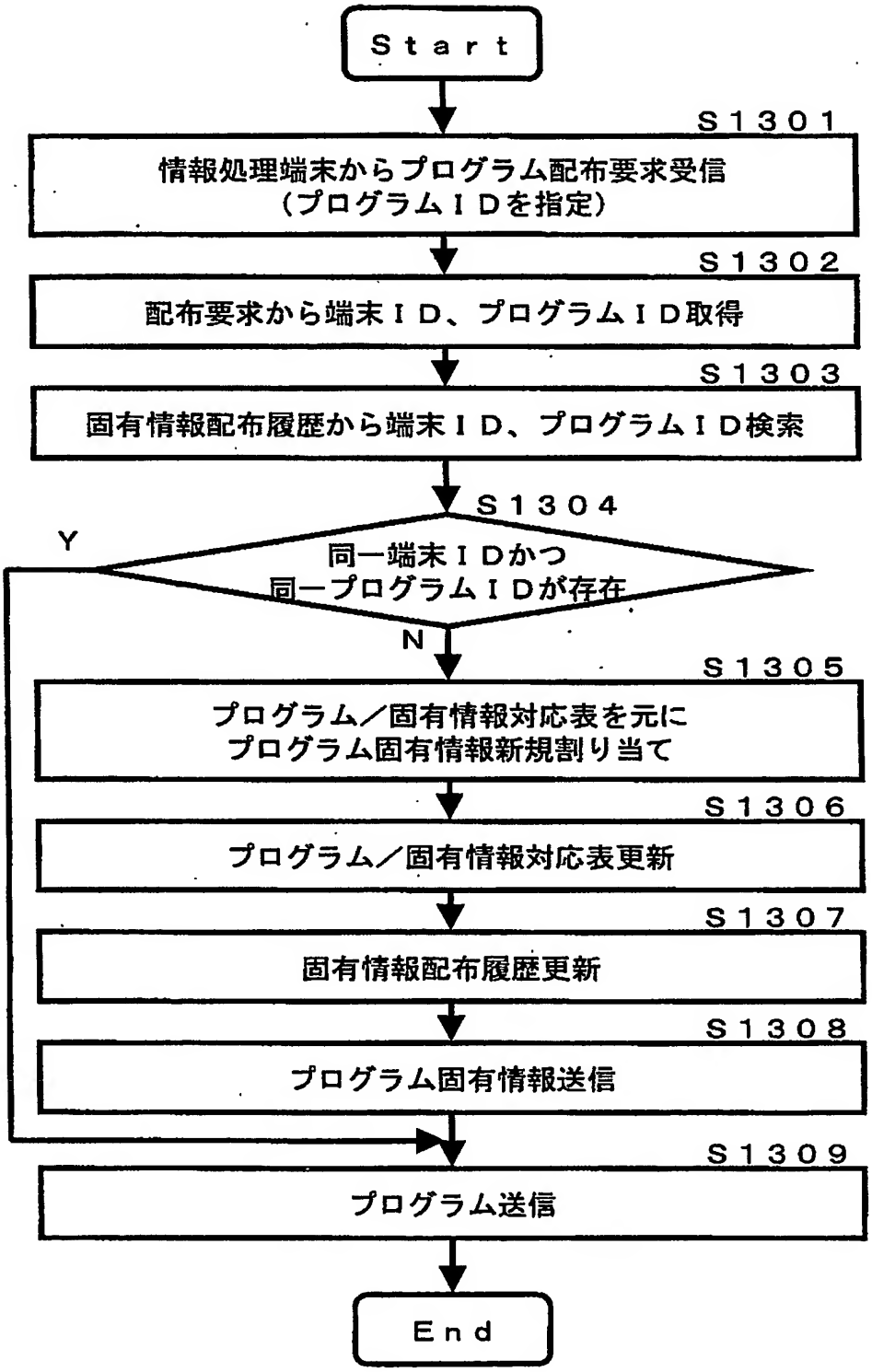
固有情報配布履歴 １２００

１２０１ 端末ＩＤ	１２０２ プログラムＩＤ	１２０３ プログラム固有情報ＩＤ	１２０４ 最終配布日付
０００１	０００１	０００１	２００２．３．１２
０００２	０００１	０００２	２００２．３．１２
００１０	０００１	０００３	２００２．３．１３
００１５	０００１	０００４	２００２．３．１４
００２０	０００２	１００１	２００２．３．１４

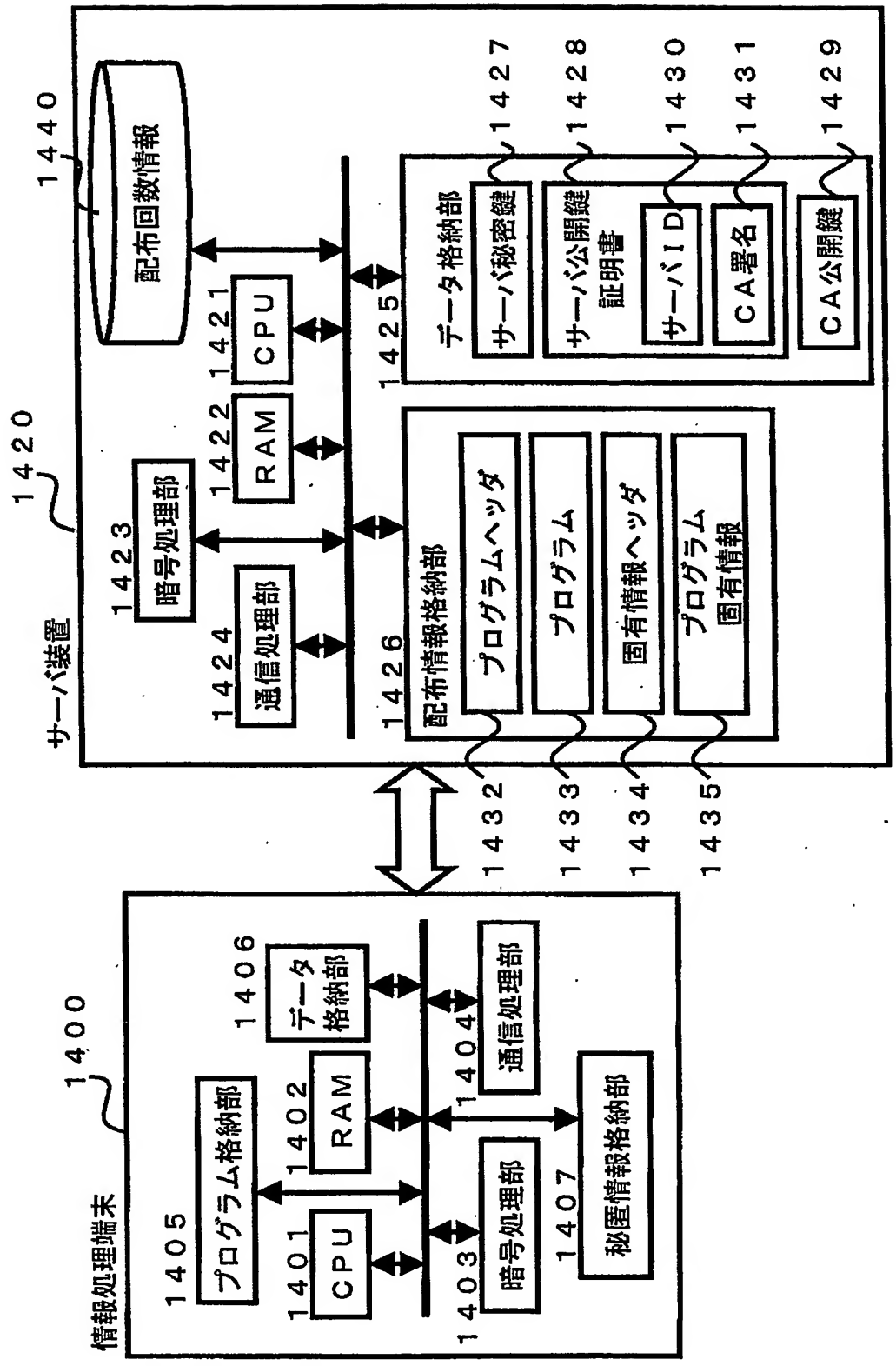
プログラム／固有情報対応表 １２１０

１２１１ プログラムＩＤ	１２１２ プログラム固有情報ＩＤ	１２１３ 配布開始ＩＤ
０００１	０００１～１０００	０１２３
０００２	１００１～２０００	１４２３
：		

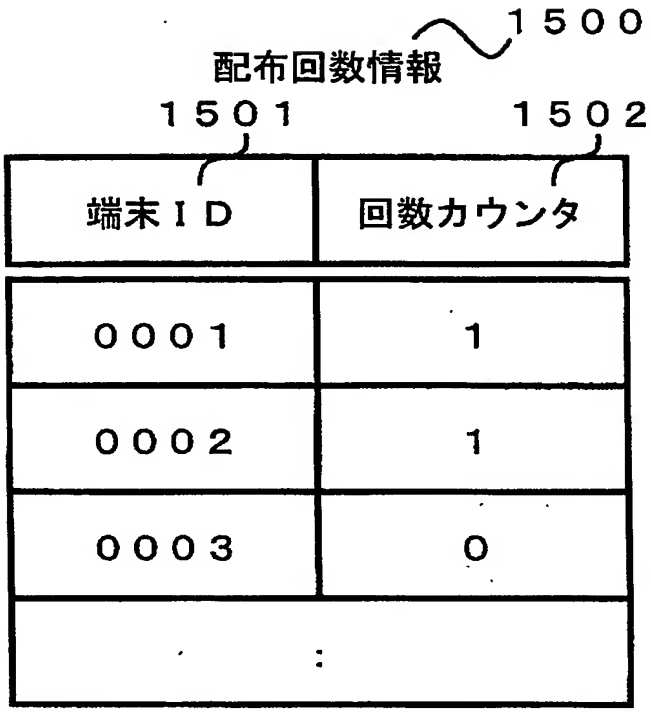
【図１３】


Ｓｔａｒｔ
Ｓ１３０１
情報処理端末からプログラム配布要求受信
（プログラムＩＤを指定）
Ｓ１３０２
配布要求から端末ＩＤ、プログラムＩＤ取得
Ｓ１３０３
固有情報配布履歴から端末ＩＤ、プログラムＩＤ検索
Ｓ１３０４
同一端末ＩＤかつ
同一プログラムＩＤが存在
Ｙ
Ｎ
Ｓ１３０５
プログラム／固有情報対応表を元に
プログラム固有情報新規割り当て
Ｓ１３０６
プログラム／固有情報対応表更新
Ｓ１３０７
固有情報配布履歴更新
Ｓ１３０８
プログラム固有情報送信
Ｓ１３０９
プログラム送信
Ｅｎｄ

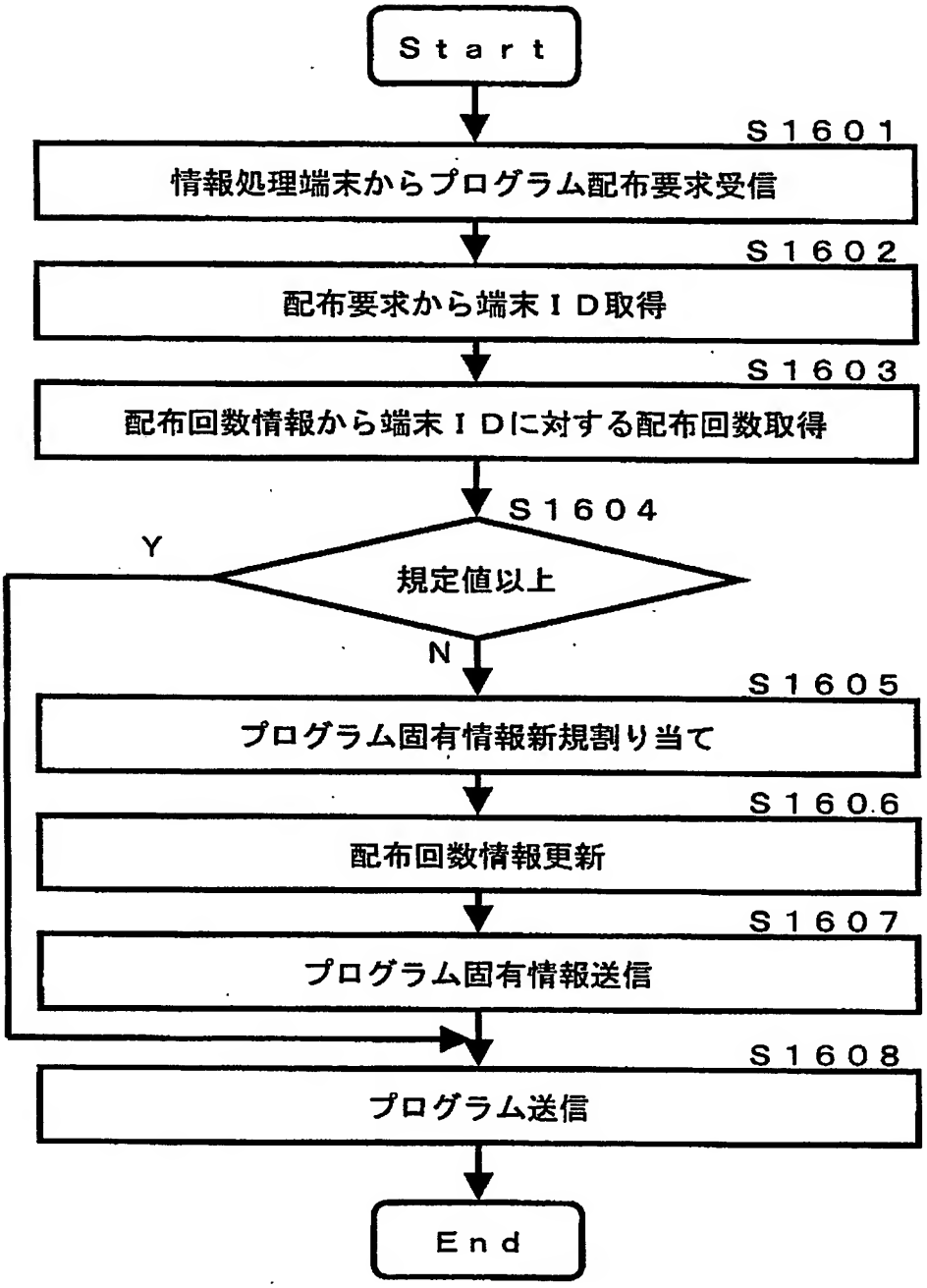
【図１４】


情報処理端末
1400
CPU
1401
RAM
1402
暗号処理部
1403
通信処理部
1404
データ格納部
1406
プログラム格納部
1405
秘匿情報格納部
1407
1432
1433
1434
1435
サーバ装置
1420
配布回数情報
1440
CPU
1421
RAM
1422
暗号処理部
1423
通信処理部
1424
配布情報格納部
1426
プログラムヘッダ
プログラム
固有情報ヘッダ
プログラム固有情報
データ格納部
1425
サーバ秘密鍵
1427
サーバ公開鍵証明書
1428
サーバID
1430
CA署名
1431
CA公開鍵
1429

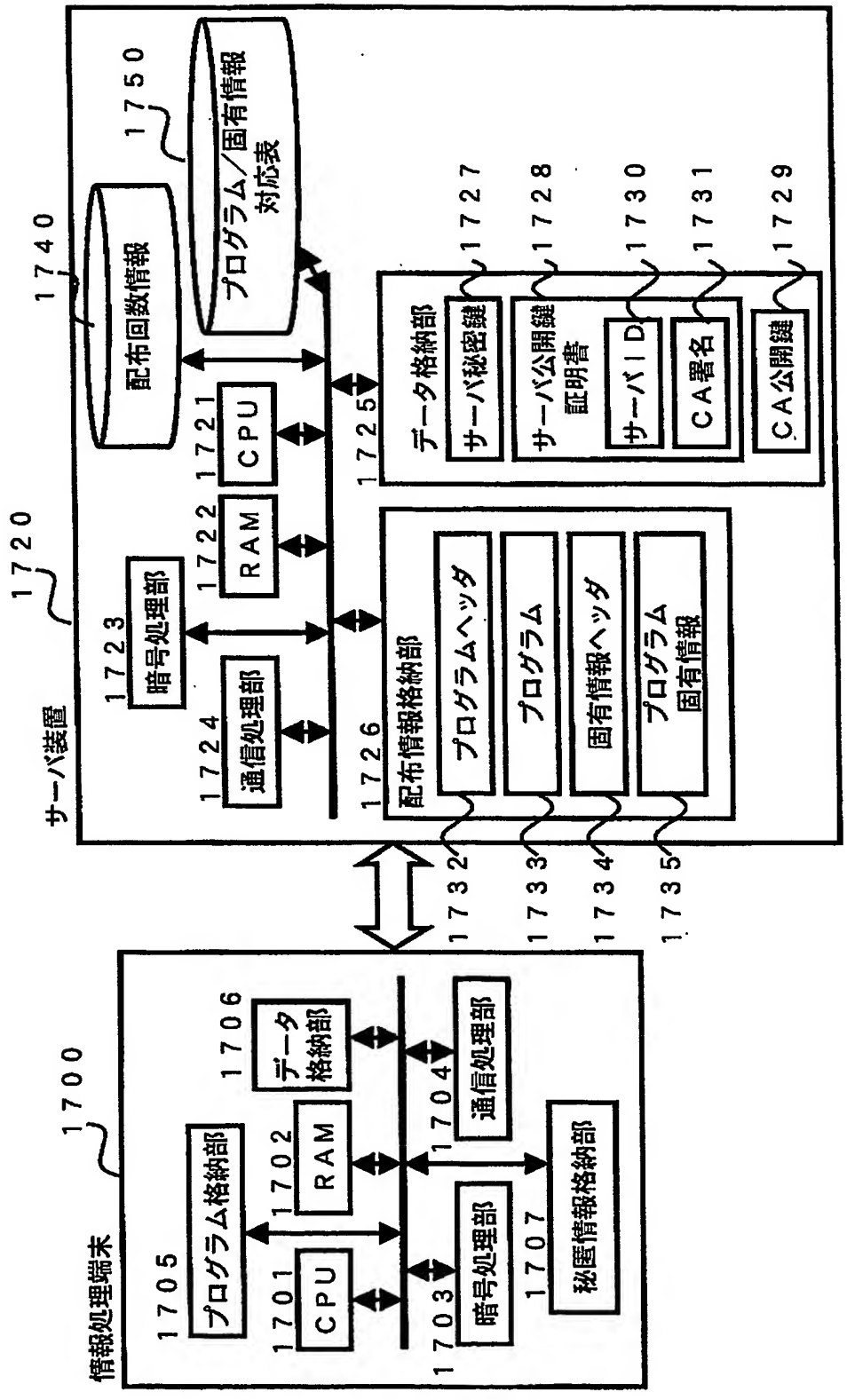
【図１５】



【図１６】


Ｓｔａｒｔ
Ｓ１６０１
情報処理端末からプログラム配布要求受信
Ｓ１６０２
配布要求から端末ＩＤ取得
Ｓ１６０３
配布回数情報から端末ＩＤに対する配布回数取得
Ｓ１６０４
Ｙ
規定値以上
Ｎ
Ｓ１６０５
プログラム固有情報新規割り当て
Ｓ１６０６
配布回数情報更新
Ｓ１６０７
プログラム固有情報送信
Ｓ１６０８
プログラム送信
Ｅｎｄ

【図１７】


サーバ装置
1720
1740
配布回数情報
1750
プログラム／固有情報対応表
1721
CPU
1722
RAM
1723
暗号処理部
1724
通信処理部
1725
データ格納部
1727
サーバ秘密鍵
1728
サーバ公開鍵証明書
1730
サーバＩＤ
1731
ＣＡ署名
1729
ＣＡ公開鍵
1726
配布情報格納部
プログラムヘッダ
プログラム
固有情報ヘッダ
プログラム固有情報
1732
1733
1734
1735
情報処理端末
1700
1701
CPU
1702
RAM
1703
暗号処理部
1704
通信処理部
1705
プログラム格納部
1706
データ格納部
1707
秘匿情報格納部

【図１８】

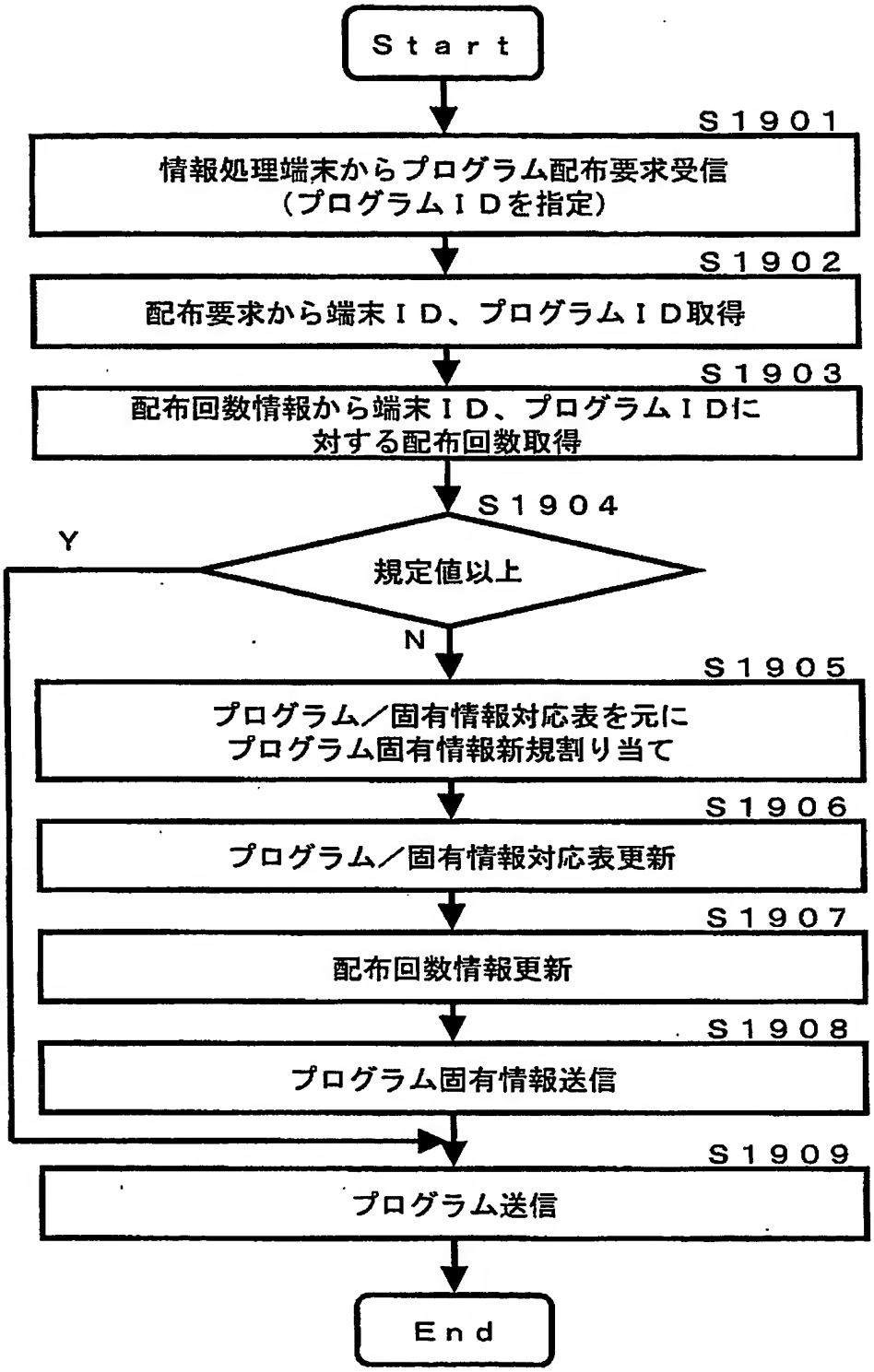
配布回数情報 1800

プログラムＩＤ (1801)	端末ＩＤ (1802)	回数カウンタ (1803)
０００１	０００１	1
０００１	０００２	1
０００１	０００３	0
０００２	０００１	1
０００２	０００２	0
０００２	０００３	0
:		

プログラム／固有情報対応表 1810

プログラムＩＤ (1811)	プログラム固有情報ＩＤ (1812)	配布開始ＩＤ (1813)
０００１	０００１～１０００	０１２３
０００２	１００１～２０００	１４２３
:		

【図１９】


Ｓｔａｒｔ
Ｓ１９０１
情報処理端末からプログラム配布要求受信
（プログラムＩＤを指定）
Ｓ１９０２
配布要求から端末ＩＤ、プログラムＩＤ取得
Ｓ１９０３
配布回数情報から端末ＩＤ、プログラムＩＤに
対する配布回数取得
Ｓ１９０４
規定値以上
Ｙ
Ｎ
Ｓ１９０５
プログラム／固有情報対応表を元に
プログラム固有情報新規割り当て
Ｓ１９０６
プログラム／固有情報対応表更新
Ｓ１９０７
配布回数情報更新
Ｓ１９０８
プログラム固有情報送信
Ｓ１９０９
プログラム送信
Ｅｎｄ

【書類名】　要約書

【要約】

【課題】　プログラムをサーバ装置から配布する場合に、サーバ装置の負担を軽減し、プログラムの不正コピーや不正改ざんを防ぐと共に、不正行為を防止することが可能なプログラム更新及び管理方法を提供する。

【解決手段】　サーバ装置から配布されたプログラムを情報処理端末において、端末毎に異なる固有鍵で暗号化して格納する。このとき、平文プログラムのハッシュ値を用いて固有鍵への暗号化が正常に行えたことを確認する。また、固有情報配布履歴をサーバ装置が保持することにより、複数のプログラム固有情報を１台の情報処理端末に配布することを防ぎ、不正行為を防止することが可能となる。

【選択図】　図１１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社